Safeguards and Security

Qualification Standard

Reference Guide

OCTOBER 2010

This page is intentionally blank.

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Tables

Acronyms	
ACL	access control list
ACREM	accountable classified removable electronic media
AEA	Atomic Energy Act
AHWG	ad-hoc working group
AIP	Aviation Implementation Plan
ALARA	as low as is reasonably achievable
ANACI	access national agency check and inquiries
AR	administrative review
ARAPT	alarm response and assessment performance tests
ASD	adversary sequence diagram
ASSESS	analytic system and software for evaluating safeguards and security
ASTM	American Society for Testing and Materials
ATOMAL	"Restricted Data" or "Formerly Restricted Data" (term used only by NATO)
BBs	ball bearings
BMS	balanced magnetic switch
C	confidential
CA	closed area
CAS	central alarm stations
C&A	certification and accreditation
CBK	common body of knowledge
CBW	chemical/biological weapons
CDP	critical detection point
CE	capital expense
C/FGI-Mod	confidential foreign government information modified handling
CFR	Code of Federal Regulations
CFX	command field exercise
CI	counterintelligence
CIO	Chief Information Officer
CM	configuration management
CMPC	classified matter protection and control
CNSS	Committee on National Security Systems
CoL	consequence of loss
COEI	composition of ending inventory
CPCI	Central Personnel Clearance Index
CPI	critical program information
CPX	command post exercise
CQB	close quarters battle
CRD	contract requirements document
CRD	confidential restricted data
CREM	classified removable electronic media
CS	cyber security

Acronyms	
C/S	confidential/secret
CSA	cognizant security authority
CSCS	contract security classification specification
CSPP	Cyber Security Program Plan
CTA	central technical authority
CUI	controlled unclassified information
DAA	designated approving authority
DBT	design basis threat
DEAR	DOE Acquisition Regulation
DCID	Director of Central Intelligence Directive
DMC	dye marking cartridge
DNA	does not apply
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DRP	disaster recovery plan
DSS	Defense Security Service
E	Excluded Parent
EA	exclusion area
EM	emergency management
EMT	emergency management team
EO	Executive Order
EOC	emergency operations center
EOD	explosive ordnance disposal
ES&H	environment, safety, and health
ESM	electronic storage media
ESS	engagement simulation system
FA	Federal agent
FACTS	Foreign Access Central Tracking System
FAQS	functional area qualification standard
FBI	Federal Bureau of Investigation
FCL	facility clearance
FDAR	facility data and approval record
FGI	foreign government information
FIPS	Federal Information Processing Standard
FISMA	Federal Information System Management Act
FLETC	Federal Law Enforcement Training Center
FO	Federal officer
FOCI	foreign, ownership, control, or influence
FoF	force-on-force
FPF	Federal protective force

Acronyms	
FRD	formerly restricted data
FSO	facility security officer
GAO	Government Accountability Office
GPP	general plant project
GRS	general records schedule
GSA	General Services Administration
GSP	graded security protection
GSS	general support systems
HQ	headquarters
HRP	Human Reliability Program
IAEA	International Atomic Energy Agency
IATO	interim authority to operate
IATT	interim approval to test
ICT	inventory change type
IDS	intrusion detection system
IDAS	intrusion detection and assessment systems
IG	Office of Inspector General
IMI	impact measurement index
INFOCON	information condition
IP	information protection
IPSEC	internet protocol security
ISA	interconnection security agreement
ISE	information sharing environment
ISM	integrated safety management
ISSM	integrated safeguards and security management
IT	information technology
ITSEC	information technology security evaluation criteria
JA	job analysis
JCATS	joint conflict and tactical simulation
JTS	joint tactical simulation
JTX	joint training exercise
KMP	key management personnel
KSA	knowledge, skill, and ability
LA	limited area
LAN	local area network
LEA	law enforcement agencies
LICP	line item construction project
LOI	Letter of Interrogatory
LSPT	limited scope performance test
MA	material access
MAA	material access area

Acronyms	
MAP	major application
MBA	material balance area
MBR	material balance report
MC&A	material control and accountability
MILES	multiple integrated laser engagement systems
MOU	memorandum of understanding
NACC	national agency check with credit
NACLC	national agency check with law and credit
NARA	National Archives and Records Administration
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NFPA	National Fire Protection Association
NISP	National Industrial Security Program
NIST	National Institute of Standards and Technology
NMC	nuclear materials courier
NMMSS	nuclear materials management and safeguards systems
NMR	nuclear materials representative
NNSA	National Nuclear Security Administration
NOFORN	no foreign
NP	non-possessing
NR	not rated
NRC	Nuclear Regulatory Commission
NSC	National Security Council
NSI	National Security Information
NSTISSI	National Security Telecommunications and Information Systems Security
NTC	National Training Center
NUREG	nuclear regulation
OA	Office of Independent Oversight and Performance Assurance
OC	operations center
OCI	Office of Counterintelligence
ODNCI	Office of Defense Nuclear Counterintelligence
OE	operational expense
OFI	Office of Federal Investigations
OGAs	other government agencies
OJT	on-the-job-training
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OPSEC	operations security
OSI	open system interconnection
OST	Office of Secure Transportation
OUO	official use only

Acronyms	
PA	protected area
PB	paint ball
PCSP	Program Cyber Security Plan
PDD	Presidential Decision Directive
P_E	probability of system effectiveness
PEP	performance execution plan
PERS SEC	personal security
PF	protective force
PFO	protective force operations
PIAs	privacy impact assessments
PIDAS	perimeter intrusion detection and assessment system
PIN	personal identification number
PIT	precision immobilization technique
P_N	probability of neutralization
POAM or POA&M	plan of actions and milestones
PP	property protection
PPA	property protection area
PP&M	program planning and management
PQP	professional qualification program
PRFOT	precision rifleman forward observer team
PS	physical security
PSF	personnel security file
PSI	personnel security interview
PT	performance test
RD	restricted data
RIS	reporting identification symbol
ROE	rules of engagement
ROI	report of investigation
ROWS	remotely operated weapons systems
RP	resource plan
S	secret
SA	special agent
SAP	special access program
SAPOC	SAP oversight committee
SAR	safety analysis review
SAS	secondary alarm station
SAVI	systematic analysis of vulnerability to intrusion
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facilities
SDLC	system development life cycle

Acronyms	
SECON	security conditions
SF	standard form
SIRPS	security incident response plan
SME	subject matter expert
SNM	special nuclear material
SO	security officer
SP	special publication
SPO	security police officer
SRD	secret restricted data
SRT	special response team
S&S	safeguards and security
SSBI	single scope background investigation
SSBI-PR	single scope background investigation-periodic reinvestigation
SSIMS	safeguards and security information management system
SSP	site security plan
SSSP	site safeguards and security plan
ST&E	security testing and evaluation
TAP	training approval program
TCP/IP	transmission control protocol/internet protocol
TCSEC	trusted computer system evaluation criteria
TE	tactical entry
TEC	total estimated cost
TID	tamper indicating device
TMR	technical and management requirements
TPC	total project cost
TRANSCOM	transportation command
TRF	tactical response force
TS	Top Secret
TSCP	technical surveillance countermeasure program
TSRD	top secret restricted data
(U)	unclassified (as in after a specific document)
UCNI	unclassified controlled nuclear information
UFVA	unclassified foreign visits and assignment
U.K.	United Kingdom
UL	Underwriter's Laboratory
U.S.	United States
U.S.C.	United States Code
USCIS	U.S. Citizenship and Immigration Service
USJFCOM	U.S. Joint Forces Command
VAs	vulnerability assessments
VfoF	validation force-on-force

Acronyms	
VPN	virtual private network
VTR	vault-type room
WLAN	wireless local area network
WMD	weapons of mass destruction

PURPOSE

The purpose of this reference guide is to provide a document that contains the information required for a Department of Energy (DOE)/National Nuclear Security Administration (NNSA) technical employee to successfully complete the Safeguards and Security Functional Area Qualification Standard (FAQS). Information essential to meeting the qualification requirements is provided; however, some competency statements require extensive knowledge or skill development. Reproducing all the required information for those statements in this document is not practical. In those instances, references are included to guide the candidate to additional resources.

SCOPE

This reference guide addresses the competency statements in the May 2009 edition of DOE-STD-1171-2009, *Safeguards and Security Functional Area Qualification Standard*. The qualification standard contains 67 competency statements.

Please direct your questions or comments related to this document to the NNSA Learning and Career Development Department.

PREFACE

Competency statements and supporting knowledge and/or skill statements from the qualification standard are shown in contrasting bold type, while the corresponding information associated with each statement is provided below it.

A comprehensive list of acronyms and abbreviations is found at the beginning of this document. It is recommended that the candidate review the list prior to proceeding with the competencies, as the acronyms and abbreviations may not be further defined within the text unless special emphasis is required.

The competencies and supporting knowledge, skill, and ability (KSA) statements are taken directly from the FAQS. Only significant corrections to errors in the technical content of the discussion text source material are identified. Editorial changes that do not affect the technical content (e.g., grammatical or spelling corrections, and changes to style) appear without remark. When they are needed for clarification, explanations are enclosed in brackets.

Every effort has been made to provide the most current information and references available as of October 2010. However, the candidate is advised to verify the applicability of the information provided. It is recognized that some personnel may oversee facilities that utilize predecessor documents to those identified. In those cases, such documents should be included in local qualification standards via the Technical Qualification Program.

In the cases where information about a FAQS topic in a competency or KSA statement is not available in the newest edition of a standard (consensus or industry), an older version is referenced. These references are noted in the text and in the bibliography.

TECHNICAL COMPETENCIES

A. SAFEGUARDS AND SECURITY PROGRAM PLANNING AND MANAGEMENT (PP&M)

1. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the standardized approach for protection program planning that will provide an information baseline for use in integrating Departmental Safeguards and Security (S&S) considerations, facilitating management evaluation of program elements, determining resources for needed improvements, and establishing cost-benefit bases for analyses and comparisons.

a. Discuss the essential elements for planning of S&S programs.

The following is taken from DOE M 470.4-1 chg 1.

The following are essential elements for planning of S&S programs:

S&S Philosophy

S&S interests and activities must be protected from theft, diversion, terrorist attack, industrial sabotage, radiological sabotage, chemical sabotage, biological sabotage, espionage, unauthorized access, compromise, and other acts that may have an adverse impact on national security; the environment; or pose significant danger to the health and safety of DOE Federal and contractor employees or the public. DOE protective forces (PFs) that protect category I quantities of special nuclear material (SNM); credible rollup of SNM to a category I quantity; or those facilities that meet or exceed the threat level 2, must employ the DOE tactical doctrine found in DOE M 470.4-1 chg 1, *Safeguards and Security Program Planning and* Management, appendix 2 of section A.

S&S Management Plan

This plan must provide a description of the implementation of S&S policy and provide detailed information on the assignment of roles, responsibilities, and authorities, as well as the development of budgets and allocation of resources. The S&S management plan must be updated annually (at least every 12 months) and must document

- roles, responsibilities, delegations, and authorities for the S&S program
- organizational structure and accountability
- planning and budget (including personnel resources)

S&S Program Operations

Actions must be taken to ensure an acceptable S&S program, including curtailment or suspension of operations when such operations would result in an immediate and unacceptable impact to national security, the environment, or the health and safety of the public or employees.

Site-Specific Characterization

Protection programs must be tailored to address specific site characteristics and requirements, current technology, ongoing programs, and operational needs to achieve acceptable protection levels that reduce risks in a cost-effective manner.

Threat Policy/Guidance

DOE O 470.3A (archived), *Design Basis Threat Policy*, must be used with local threat guidance during the conduct of vulnerability assessments (VAs) for protection and control program planning. The design basis threat (DBT) must be the baseline threat definition but local threat guidance may be used to increase the level of threat to be analyzed.

Targeted Protection Strategies

- Strategies for the physical protection of SNM and vital equipment must incorporate the applicable requirements established in DOE M 470.4-2A, *Physical Protection*.
- Protection strategies must be implemented as specified in the DBT. PF resources must focus on decisively defeating the terrorist threat, which is facilitated by positioning posts so there is little or no delay in responding to critical targets, eliminating posts which detract from constant readiness, and maximizing use of physical protection systems to enhance PF effectiveness. PF resources must be positioned to interdict and neutralize the adversary threat as far as possible outside the boundaries of the target location.
- Protection program elements must be designed to prevent and/or mitigate the consequences of acts of radiological, chemical, or biological sabotage that would cause unacceptable impact to national security, the environment, or the health and safety of the public or employees. Protection elements, such as active denial systems, must be designed and deployed to minimize the need for PF recapture/recovery operations.
- Strategies for the protection and control of classified information or matter must incorporate the applicable requirements established in DOE M 470.4-4A, *Information Security Manual*.
- Security systems must be used that prevent, detect, or deter unauthorized access, modification, or loss of classified and unclassified controlled matter and its unauthorized removal from a site or facility.
- Strategies for the protection of government property not covered above must reflect a graded approach. DOE offices, facilities, and property protection areas (PPAs) must meet or exceed General Services Administration (GSA) minimum security standards.
- Security countermeasures for explosive threats must address a range of activities including hand-carried, mailed, and vehicle-transported devices.

Graded Protection

The Department recognizes that risks must be accepted; however, an acceptable level of risk must be determined based on evaluation of a variety of facility-specific goals and considerations. By a graded approach, the Department intends that the highest level of

protection be given to security interests and activities whose loss, theft, compromise, and/or unauthorized use would seriously affect the national security, the environment, departmental programs, and/or the health and safety of the public or employees. Protection of other interests and activities must be graded accordingly.

Risk Management

S&S programs must be based on the results of vulnerability and risk assessments, the results of which are used to design and provide graded protection according to an asset's importance or the impact of its loss, destruction, or misuse. The results of the assessments, to include the determination of system effectiveness, are one of the key considerations the manager must evaluate when establishing the level of risk. For example, if it is determined that there is high risk that is not being mitigated by compensatory measures, reporting must be made to the Secretary of Energy or the Deputy Secretary who can accept high risk. Cognizant under secretaries can accept moderate risk.

- Vulnerability and risk assessments must be conducted and documented to support the identification of risks to be accepted by the Department.
- To determine the appropriate level of protection against risk, line management must consider the threat, the vulnerability of the potential target, and the potential consequences of an adversarial act.

Site-Specific Programs

- S&S programs must address site-specific characteristics.
- Performance assurance programs must be developed, managed, and implemented to ensure that S&S programs and protection program elements protect security interests and activities. These programs must ensure intensive, frequent performance testing of PF individuals and unit tactics with oversight by line management and independent oversight organizations.
- A management and planning process to achieve integrated, site-specific protection from unauthorized actions must be implemented. This process must be based on a graded approach that implements the integrated concepts of deterrence, prevention, detection, and response.
- The DBT must be used as the basis for planning protection programs.

b. Discuss the types of facilities for which S&S plans must be developed.

The following is taken from DOE M 470.4-1 chg 1.

S&S plans must be developed for facilities with any of the following S&S interests:

- Category I quantities of SNM or credible roll-up quantities of SNM to a category I quantity
- Category II, III, or IV SNM
- Radiological, chemical, or biological sabotage threats
- Critical mission disruption threats
- Intra-/inter-site transportation of SNM

- Classified information or matter
- Facilities engaged in the protection of government property
- Facilities that the Secretary, Deputy Secretary, or under secretaries deem appropriate

c. Discuss the difference between the Site Safeguards and Security Plan (SSSP) and the Site Security Plan (SSP).

The following is taken from DOE M 470.4-1 chg 1.

The SSSP is a five-year master planning document that must be prepared for sites with facilities described in DOE M 470.4-1 chg 1, paragraphs 3a(1), (3), (4), or (8). The SSSP must depict the existing condition of site protection programs and, when the DBT performance standard cannot be met, establish improvement priorities and resource requirements for the necessary improvements.

At locations where an SSSP is not required because of the limited scope of interests, an SSP must be developed to describe the protection program. SSPs must be approved by the local DOE cognizant security authority (CSA). In addition, specialized plans must be developed to address protection programs for other protection operations. Requirements for specialized plans that may or may not be components of the SSP are set forth in the applicable DOE directives.

d. Discuss the documents that must be used to support program forecasts and information input used in the protection program planning process.

The following is taken from DOE M 470.4-1 chg 1.

The documents listed below must be used to support program forecasts and information input used in the protection program planning process:

- Applicable departmental directives, guidance, and intelligence assessment information developed and disseminated by line management of the Office of Security
- Programmatic guidance and forecasts of significant changes planned in site operations as communicated through line management
- Current and projected operational constraints and resources
- Analysis of cost and effectiveness of security technologies versus traditional protection methodologies

e. Discuss the plan review and approval process.

The following is taken from DOE M 470.4-1 chg 1.

The SSSP requires approval by DOE line management and concurrence by the cognizant head of the departmental element (see DOE M 470.4-1 chg 1, attachment 1). Such approval authority must be formally delegated to line management.

- Copies of approved SSSPs must be provided to the Office of Security for review and comment.
- Other security plans may be approved as stipulated in the applicable directive. If approving authority is not otherwise stipulated, these security plans may be approved by DOE line management.

The SSSP must be submitted to DOE line management within 150 days of the termination date of data collection and approved within 120 days of the submittal date. Directive changes, facility reconfiguration, a new VA, or other activities that occur after the stated effective date will not be considered for purposes of reviewing/approving the plan.

The SSSP must be reviewed annually (at least every 12 months). Updates to the SSSP that may significantly alter the agreed-upon protection philosophy or performance standards of protection systems must be subjected to the formal VA process, and if changes are shown to significantly alter system effectiveness performance, the update(s) will be subject to the same concurrence and approval as stated in DOE O 470.4-1 chg 1, paragraph 3e(1).

An information copy of approved modifications must be provided to the Office of Security.

f. Discuss the parts of the S&S Management Plan.

The following is taken from DOE M 470.4-1 chg1.

The S&S management plan provides a description of the implementation of S&S policy and provides detailed information on the assignment of roles, responsibilities, and authorities, as well as the development of budgets and allocation of resources. The following outline delineates the content requirements and provides a suggested format for the S&S management plan.

Executive Summary

- Program mission statement. Briefly describe the program mission and how the mission relates to national security. Describe the major elements or activities performed in terms of program mission and its relationship to the DOE national security mission.
- S&S program structure. Briefly describe the strategy and organizational elements used to implement the S&S program under their cognizance.
- Management and planning assumptions. Briefly describe those assumptions that affect the management and planning of the implementation of the S&S program. (e.g., items such as the following):
  - Future of the program (mission, staffing levels, site status, etc.)
  - Current and planned S&S projects
  - Status of the organization's S&S budget

Part 1—Organizational Structure and Accountability

- Line management organization. Describe the structure and relationship of line management. Identify the roles, responsibilities, and authorities of these line management elements to include organizational charts.
- CSA organization. Describe the structure of line management that is specifically responsible for implementing the departmental element's S&S program. Identify the individuals and positions responsible for committing resources and directing the activities of personnel associated with the S&S program.
    - Headquarters organizational structure. For the headquarters elements, provide an organizational chart to show the S&S organization and management structure and the lines of authority and points of interface with other programs which affect S&S. Describe the functions and responsibilities of S&S personnel and indicate how S&S activities are integrated with those of other facility organizations; include organizational responsibilities for line management overseeing the program as well as the interface points with the respective departmental element.
    - Field organizational structure. For the field elements, provide an organizational chart to show the S&S organization and management structure and the lines of authority and points of interface with other programs which affect S&S. Describe the functions and responsibilities of S&S personnel and indicate how S&S activities are integrated with those of other facility organizations; include organizational responsibilities for line management overseeing the program as well as the interface points with the respective departmental element.
- Contractor sites. Provide the contract name, number, and other information that describes the authority under which the contractor executes management functions for facilities under the cognizance of a departmental element. Identify the site contractor elements responsible for S&S programs and describe their S&S activities. Provide Federal and contractor organization charts and identify key positions and the relationships between the organizations responsible for S&S activities. Describe Federal and contractor involvement in the development of S&S resource requirements.

Part 2—Roles, Responsibilities, Delegations, and Authorities. Delegations must be documented in writing and delineate all assigned S&S roles, responsibilities, and authorities for the S&S program. This section should include the following:

- Documents offices/positions affected by the S&S Management Plan
- Establishes the approval chain for S&S plans, procedures, and implementation policy
- Establishes the approval chain for S&S policy deviations
- Assigned reporting requirements for incidents of security concern
- A list of roles and responsibilities for key positions and the delegated authorities for each

Part 3—S&S Program Implementation. This section of the S&S management plan documents the processes and methods used to implement the Department's security policies. This section identifies the following:

- Methods used for ensuring all applicable programmatic requirements are implemented throughout the organizational element
- Methods used for ensuring effective integration of S&S programmatic elements
- SSSPs and SSPs used to implement S&S policy requirements

Part 4—Planning and Budget (including personnel resources). This section of the S&S management plan documents the key processes of planning and budgeting, including strategic planning, budget formulation, budget execution, and program evaluation.

- Describe the strategic planning assumption used to ensure the S&S program will meet mission objectives.
- Provide a five-year plan that describes the budget formulation priorities for future S&S resources and programs.
- Provide the current year plan for executing the S&S budget. This plan details the allocation of resources that support S&S functions and missions.
    - Provide a program evaluation plan that details how the CSA will assess the implementation of the S&S program and the organization's progress toward meeting established missions/goals. The program evaluation plan must cover both the Federal and contractor elements of the departmental element. This plan can be used to support award fee decisions by the departmental element.
    - Briefly describe any changes to operational requirements which affect S&S program operations or would require increments or decrements to operational accounts.

g. Describe the DOE's fundamental approach to protecting nuclear weapons and components, Special Nuclear Material (SNM), or targets subject to radiological or toxicological sabotage.

The following is taken from DOE M 470.4-1 chg 1.

The establishment of departmental doctrine governing the defense of sensitive national security assets is necessary to ensure the uniform application of effective security measures throughout the complex. DOE M 470.4-1 chg 1, appendix 2 is the condensed expression of the Department's fundamental approach to protecting nuclear weapons and components, SNM, or targets subject to radiological or toxicological sabotage. In keeping with the development of higher standards for individual training and fitness, aggressive small unit tactics must be employed within the bounds of a well-defined and constructed area defense that is supported by fixed strong points, obstacles/barriers, advanced detection and assessment capabilities, coordinated fire planning, updated weapons systems, and armored vehicles.

h. Discuss the purpose of an armed Protective Force (PF).

The following is taken from DOE M 470.4-1 chg 1.

Within DOE, armed PFs exist to deter and to defeat terrorist or other adversarial actions that could have major national security consequences; primarily, unauthorized access to nuclear weapons and components, SNM, or targets subject to chemical, biological, or radiological sabotage or that contain a unique capability that must be protected. When availability of armed PFs is limited, they shall not be used to:

- perform routine, repetitive tasks that are not related directly to target protection;
- perform access control functions that can be better accomplished through automation;
- act as administrative escorts for construction projects or service personnel (unless required for protection of assets); or
- staff posts that offer convenience to management and/or employees.

i. Describe the concept of the Tactical Doctrine.

The following is taken from DOE M 470.4-1 chg 1.

In general, at category I/II facilities within the DOE, defensive plans will involve an area defense with fixed strong points, or fighting positions, that encompass a target and lie within a concentric arrangement of intrusion detection systems and barriers designed to detect, delay, and engage the adversary as far from the target as possible. A tactical response force (TRF) consisting of highly-trained, motivated, and skilled tactical units/teams will be positioned on, or in proximity to, each target. Early detection will permit interdiction by mobile response teams using fire and maneuver techniques to deny further access to adversaries and/or to channel them into attrition areas covered by interlocking bands of fire from fixed, hardened fighting positions.

j. Discuss the essential defensive planning principles.

The following is taken from DOE M 470.4-1 chg 1.

The defensive planning principles include the following:

- Prepare the defensive area.
  - Prepare a barrier plan.
    - Minimize the number of access points and/or avenues of approach.
    - Channel the adversary into attrition areas by use of barriers and preplanned, interlocking bands of fire.
    - Channel the high ground, either by physical presence or by weapons fire.
  - Prepare a defensive fire plan that ensures the following:
    - Clear fields of fire and observation across the battlefield are maintained.

- Defensive positions are mutually supporting.
- High volumes of fire can be brought onto key terrain features, obstacles, and along expected routes of approach.
- The volume of fire brought upon an adversary increases as a target area is approached.

- Integrate all aspects of the defensive plan.
  - Employ multiple layers of detection.
  - Employ multiple layers of delay (e.g., barriers/obstacles).
  - Integrate technology, such as remotely operated weapon systems (ROWS), active denial systems, and advanced detection and observation systems, with response force tactics.
  - Ensure that barriers are covered by weapons fire.
  - Ensure that the entire defensive perimeter is covered by interlocking fields of fire from mutually supporting positions.
  - Where feasible, control the configuration of the battlefield by eliminating anything that could provide potential adversary cover and/or concealment.
  - Ensure that likely avenues of approach are defended with sufficient force to compel a decisive engagement with the adversary.
  - Protect defenders by employing hardened fighting positions situated for mutual support.
  - Establish supplementary defensive positions.
  - Prepare to maneuver offensive forces to attack and to defeat an adversary whose progress is delayed by engagement with defensive fire.
- Make the adversary fight to the target.
  - Adversary detection and engagement must occur as far from the target as possible.
  - Assign sufficient resources to be able to assess remote alarms to identify the number of adversaries, thereby helping to differentiate between diversionary attacks and the main force.
  - Plan for staged withdrawal of forces dispatched to assess remote alarms to prepared supplementary defensive positions.
  - Plan for overwatch of assessment forces with long-range weapons from within the defensive perimeter.
  - Coordinate barrier and fire control planning to ensure that the adversary will be subjected to high volumes of fire in exposed positions prior to entry into the defensive perimeter.
  - Ensure adequate standoff for vehicle-borne improvised explosive devices.
  - Limit the ability of airborne improvised explosive devices to impact key defensive positions and primary target buildings.
- Make the target location deadly.
  - Use technology to distract, interrupt, disable, or neutralize anyone who has obtained unauthorized access to target locations.

- Include considerations for re-entry and recapture of target locations in all barrier and response plans.

- Manage the site population.
  - Limit the number of personnel, vehicles, and equipment in the target area at all times.
  - Develop formal site-specific procedures for the disposition of workers in the event of an attack.

    - If the tactical conditions permit, workers may be evacuated to safe areas from prospective target locations and likely avenues of approach.
    - Sheltering in place may be the best option. Workers should be provided with specific instructions, such as to remain off the phone unless they possess information about the event, to lie on the floor, and, if PF enter their location, to keep their hands and security badges visible.

k. Discuss the elements of the Tactical Response Force (TRF).

The following is taken from DOE M 470.4-1 chg 1.

The TRF is deployed in a strategic posture to interrupt, interdict, deny, and neutralize an adversary force attack. The TRF is armed and equipped with state-of-the-art weaponry, tactical equipment, vehicles, and communication systems. The TRF is adept at implementing approved security incident response plans under adverse emergency conditions. The primary mission of the TRF is the protection of nuclear weapons, weapons components, and SNM from theft, sabotage, and unauthorized control. Ancillary duties include the safeguarding of classified information and other classified assets.

The characteristics of TRF include the following:
- Survivability
- Mobility
- Lethality
- Flexibility
- Speed
- Unpredictability
- Mutual support
- Reliable communications

A site TRF is composed of small units/teams of no fewer than two special police officers (SPO) II and/or SPO III personnel deployed in configurations that provide tactical advantages for both defensive and offensive operations.
- Special response team (SRT)—executes recapture/recovery and pursuit operations and supports interruption, interdiction, neutralization, containment, and denial strategies. SPO III qualified personnel are deployed as one or more dedicated teams

with specialized weapons and equipment, operating from mobile tactical vehicles, as ground assault forces, or a combination of both.

- Security police officer II—executes interruption, interdiction, neutralization, containment, and denial strategies and supports recapture/recovery and fresh pursuit operations. SPO II personnel operate in small units with specialized weapons and equipment from mobile patrols/tactical vehicles and fixed posts.

All site SPOs and security officers (SOs) have a key role in supporting the overall site security posture and the TRF.

- Security police officer I—supports interruption, interdiction, neutralization, containment, and denial strategies. SPO I personnel operate from mobile patrols and fixed posts. SPO I personnel perform routine S&S-related functions and are capable of performing specialized active defense functions such as staffing defensive fighting positions, operating ROWS, and performing central alarm stations (CAS) duties.
- Security officer—ensures routine security-related functions are maintained. Unarmed SOs perform observation and reporting activities, logistical re-supply to other PF elements, message courier duties, and provide transportation support.

Deployment considerations:

- A layered, or zone, defensive strategy is implemented that maximizes the TRF's ability to detect, engage, and neutralize adversary forces as they move toward a target location.
- Fixed, reinforced fighting positions, or bunkers, are utilized to enhance survivability, deny access to targets, provide overlapping fields of fire for mutual support, and to control avenues of approach.
- Protection strategies are designed to reduce predictability of the response.
- Small units/teams of no fewer than two SPO II and/or SPO III personnel are deployed in configurations that provide tactical advantages for both defensive and offensive operations.
- Personnel who will occupy fixed fighting positions, those who will perform as the flexible maneuver elements, and those who will, if required, conduct recapture/recovery operations are identified.
- Each TRF member is issued at least one primary weapon along with a secondary firearm, such as a handgun, used principally for close quarters engagement or for transition in the event of a stoppage of the primary weapon.
- TRF weapons are capable of tactical operations in both day and night conditions.
- The TRF employs direct-fire weapons to engage and to neutralize adversary forces out to the maximum effective range of the weapon.
- As prescribed by the SSSP, the TRF employs indirect-fire or explosive projectile weapons to deny access to target locations and to suppress and to neutralize adversary forces occupying positions of cover and/or concealment.
- TRF members are knowledgeable of adversary attack methods identified in the DBT and critical pathways documented in site-specific vulnerability assessment reports.

- A secure tactical command post is identified to ensure that command, control, and communications links are maintained and that backup systems are available.
- Command and control is structured down to the lowest unit/team level. Operational control of forces includes organizing and employing of forces, designating combat objectives, assigning individual and unit tasks, and issuing orders and directions necessary for mission accomplishment.
- Accurate adversary and battle information is relayed to command/control centers as it occurs.
- A system for identification, friend or foe is employed to minimize incidents of casualties from "friendly fire."

Denial strategy implementation:

- Early warning system technologies are emplaced to detect and to assess adversary movement as far as possible from target locations.
- Highly mobile tactical vehicles mounted with light and/or heavy weapon systems are deployed to support combat operations, conduct reconnaissance operations, control avenues of approach, maneuver to suppress and destroy hostile threats, and to provide mutual support for other tactical vehicles.
- A commander is designated for each tactical armored vehicle.
- Potential target access points are covered by suppressive fire weapons.
- TRF members utilize positions of cover and maximize the element of surprise to the extent possible.
- The TRF initiates a decisive engagement with adversary forces as far as possible outside the target location.
- Once an adversary has been identified and engaged, TRF elements never lose contact.
- Adversaries are engaged while they negotiate obstacles, deploy from vehicles, and cross open ground.
- TRF teams, using suppressive fire weapons, maneuver in force against adversaries occupying covered positions.
- The TRF has plans in place to transition quickly from defensive to offensive operations.

Recapture/Recovery operations:

- The site PF is staffed and deployed in sufficient strength to ensure the protection of sensitive assets. The dedicated recapture/recovery element of the SRT is established with additional resources sufficient to ensure that recapture/recovery capabilities continue to exist in the event that the denial strategy fails.
- SRT training is focused on site-specific targets and ensures that SRTs are adequately prepared to conduct recapture/recovery operations within identified target locations.
- SRTs possess the tactics, tools, and techniques necessary to gain entry, neutralize the adversary threat, control the situation, and secure national security assets.
- If hostages are involved and SNM is at risk, regaining control of the SNM is the primary consideration.

- SRTs are supported by other TRF elements to the maximum extent possible as they move toward the target objective.
- TRF members provide overwatch for the assault team(s) movement, cover avenues of approach, and provide support by fire to the SRT as they breach/enter the target location.
- All TRF personnel are capable of providing direct support to the recapture/recovery mission by supplementing the main assault force, controlling the target area, and suppressing enemy defensive positions.

Pursuit operations:

- TRF members are trained and equipped to conduct fresh pursuit operations, on and off DOE property according to DOE M 470.4-3A, *Contractor Protective Force*, section A, appendix A-1, *Guidelines for Legal Authority for Fresh Pursuit and Rules of Engagement*.
- Fresh pursuit operations are coordinated with responding Federal, state, and local law enforcement agencies according to approved agreements.
- TRF members use vehicle immobilization techniques and/or other means of applying deadly force to terminate the pursuit.
- TRF members maintain control of sensitive assets until relieved by cognizant Federal authorities.

Weapons of mass destruction:

- All TRF and SPO-I personnel are trained and equipped to operate within an environment where weapons of mass destruction (WMD) have been employed, (i.e., chemical, biological, or radiological weaponry). PF training programs include tactical deployment in WMD personal protective equipment.
- TRF members are able to transition to WMD fighting procedures rapidly enough so as to not weaken the overall combat posture.
- Individual tactical equipment is compatible with WMD personal protective equipment.

I. Discuss the National Industrial Security Program (NISP) and agency responsibilities.

The following is taken from DOE M 470.4-7, archived.

Executive Order (EO) 12829, *National Industrial Security Program*, 1-6-93, as amended by EO 12885, *Amendment to Executive Order No. 12829*, 12-14-93, establishes NISP to protect classified information released by Federal agencies to their contractors, directs the Secretary of Defense to issue the NISP operating manual, and makes the Director of the Information Security Oversight Office responsible for implementing and monitoring the NISP government-wide; however, DOE and Nuclear Regulatory Commission (NRC) retain authority over access to information classified under the Atomic Energy Act of 1954.

m. Discuss the following management considerations in applying the Tactical Doctrine:

- **Training and exercise requirements for armed PF and rules of engagement and use of force including rights and responsibilities of PF**
- **Planning and implementation**

The following is taken from DOE M 470.4-1 chg 1.

Training

Training is the key to a quality force, and the best form of tactical training is person-on-person, or force-on-force (FoF) engagements, on a repetitive basis. A requirement for increased FoFs for training purposes does not always have to involve the very large-scale exercises that are conducted during inspections and annual SSSP validations. Nor do they always need to occur in or around the actual facilities. Encouraging and assisting PF members to refine their individual and small unit tactical skills and to condition them to the reflex of shooting at adversaries can be facilitated with smaller scale training exercises using surrogate facilities. This will enable the Department to afford a much higher frequency of such activities because the costs in terms of facility shut down, coordination with operations, shadow force deployment, etc., will be substantially avoided. But, in order to achieve the desired results, these exercises must employ engagement simulation systems such as Multiple integrated laser engagement systems (MILES), dye marking cartridge (DMC) weapons, or hybrid DMC/MILES weapons that combine DMC for close-range and MILES for longer range.

Planning and Implementation.

There are issues that may be considered ancillary to the planning and implementation of the DOE facility defense model but that nevertheless are important to the viability of tactical planning and execution. Some factor directly into the planning process while others relate indirectly.

Examples are:

- Targets must be as small and as few as possible.
- All tactical training should simulate as closely as practicable the environment and manner in which PF personnel are expected to fight.
- Persons assigned as full-time staff PF instructors must be qualified according to the provisions of DOE M 470.4-3A, chapter II, paragraph 7.

2. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the requirements of the Homeland Security Advisory System.

a. Describe the meaning and use of threat indicators and Graded Security Protection (GSP) (formerly the Design Basis Threat [DBT]).

The following is taken from DOE M 470.4-1 chg 1.

While the GSP provides specific description of threats that all components of the S&S system must be capable of defeating, analysis of terrorism should be an ongoing process. Although each analysis relies on information included in previous assessments, judgments with respect to threats to Federal and DOE-affiliated personnel, facilities, and assets begin anew with each analysis.

Homeland security threat conditions (SECONs) are established based on the analysis of a continuous and timely flow of integrated all-source threat assessments and reporting provided to Executive Branch decision-makers. A threat indicator is a condition that, when present, increases the possibility of a terrorist incident. Seldom does one single indicator suggest that the threat is imminent; but, when a number of indicators are present, the level of concern should increase correspondingly. A decision on assigning SECONs must integrate a variety of considerations. This integration will rely on qualitative assessment, not quantitative calculation. Higher SECONs indicate greater risk of a terrorist act, with risk including probability and gravity. There can be no guarantee that, at any given SECON, a terrorist attack will not occur. An initial and important factor is the quality of the threat information itself. The evaluation of this threat information includes, but is not limited to, the following factors.

- To what degree is the threat information credible?
- To what degree is the threat information corroborated?
- To what degree is the threat specific and/or imminent?
- How grave are the potential consequences of the threat?

Local and site-specific threat analysis is a dynamic process because the threat and the countermeasures used to combat the threat are constantly changing. To keep up with possible changes in the threat, security professionals should develop a predetermined list of general and specific threat indicators. Threat indicators should be revised according to site/facility situations and needs. They should be reviewed at least every 6 months or when a significant incident or change in conditions indicates that the threat level is increasing or decreasing. Examples of threat indicators that can be used to develop a site-/facility-specific assessment are:

- International incidents or indicators against United States (U.S.) interests, personnel, or facilities.
- Domestic incidents or indicators against Federal or state interests countrywide.
- Local incidents or indicators directed against Federal or DOE interests.
- Specific targeting of DOE personnel, facilities, or materials.

b. Describe the DOE Security Conditions (SECON) system and the measures to be taken in the five levels.

The following is taken from DOE M 470.4-1 chg 1.

The DOE SECON system describes a progressive level of commonsense protective measures that may be implemented in response to a malevolent or terrorist threat to any or all DOE facilities, assets, and personnel. The purpose of the SECON system is to establish

standardized protective measures for a wide range of threats and to help disseminate appropriate, timely, and standardized information for the coordination and support of DOE crisis or contingency activities. Once a SECON level is declared, the associated protective measures should be implemented as soon as possible to the extent they apply to the individual site or facility. Cognizant security authorities must coordinate SECON status through their DOE points of contact and notify the DOE headquarters (HQ) operations center (OC) and departmental element of the site/facility SECON status. Measures associated with each SECON are not prioritized, but should be initiated concurrently, when practical.

A record of specific actions taken for each measure must be maintained. A description of each SECON, including the necessary circumstances for implementing, the impact on operations, and the purpose of each protective posture, is listed below.

SECON 5, Low Condition (Green). This condition is declared when there is a low risk of terrorist attacks. SECON 5 exists when a general threat of possible malevolent or terrorist activity exists, but warrants only a routine security posture.

SECON 4, Guarded Condition (Blue). This condition is declared when there is a general risk of terrorist attacks. SECON 4 applies when there is an increased general threat of possible malevolent or terrorist activity against personnel and facilities, the nature and extent of which are unpredictable, and circumstances do not justify full implementation of SECON 3. It may be necessary, however, to implement certain selected measures from higher SECONs to address intelligence received or to act as a deterrent. All measures selected for use under SECON 4 must be capable of being maintained indefinitely.

- Measure 1—at regular intervals, warn all personnel to report the following to security:
  - Suspicious personnel, particularly those carrying suitcases or other containers, or those observing, photographing, or asking questions about site operations or security measures
  - Unidentified vehicles parked or operated in a suspicious manner on or in the vicinity of the site or near site facilities
  - Abandoned parcels or suitcases
  - Any other activity considered suspicious
- Measure 2
  - Ensure that security personnel have immediate access to building floor plans and emergency/evacuation plans for all site facilities.
  - Ensure that security personnel are able to seal off an area immediately.
  - Ensure that key personnel required to implement security plans are on-call and readily available.
  - Maintain the site emergency management team (EMT) on 2-hour recall.
  - Expand operations security measures.
  - Exercise bomb threat procedures.
- Measure 3—secure and seal buildings, rooms, and storage areas not in regular use. Maintain a list of secured facilities.

- Measure 4—increase unannounced security spot checks (inspection of personal identification; vehicle registration; and the contents of vehicles, suitcases, briefcases, and other containers) at access points for the site and facilities.
- Measure 5—reduce the number of access points for vehicles and personnel to minimum levels consistent with the requirements to maintain a reasonable flow of traffic.
- Measure 6—as a deterrent, randomly apply measures 14, 15, 16, 17, or 18 from SECON 3, either individually or in combination.
- Measure 7—review all operation plans, personnel details, and logistics requirements that pertain to implementing higher SECONs.
- Measure 8—review security measures for critical/sensitive personnel and implement additional measures warranted by the threat and existing vulnerabilities.
- Measure 9—increase liaison with local law enforcement, intelligence community, security agencies, and the Federal Bureau of Investigation (FBI) to monitor the threat to site personnel and facilities. Notify local law enforcement agencies and the FBI concerning SECON 3 measures that, if implemented, could affect their operations in the local community.
- Measure 10—reserve for site/facility use.

SECON 3, Elevated Condition (Yellow). This condition is declared when there is a significant risk of terrorist attack. It applies when an increased and more predictable threat of malevolent or terrorist activity exists. The measures in this SECON must be capable of being maintained for lengthy periods without causing undue hardship, affecting operational capability, or aggravating relations with the local community. For measures requiring an increase in the frequency of a specific action, the new frequency is to be more often than in the lower-level security condition. In addition to the measures required by SECON 4, the following measures should be implemented.

- Measure 11—increase the frequency of warnings required by measure 1, and inform personnel of additional unclassified threat information, if available. Encourage increased community security awareness of suspicious persons, vehicles, and activities.
- Measure 12—maintain EMT personnel on 2-hour recall; periodically exercise recall to ensure readiness. Keep all other personnel involved in implementing special response/contingency plans on-call. Identify, contact, and brief specialists that may be required for unique contingencies; coordinate lines of communication.
- Measure 13—review provisions of all operation plans and orders and special operating procedures associated with implementing SECON 2.
- Measure 14—move automobiles and objects such as trash containers, newspaper boxes, crates, etc., at least 30 yards from all facilities, particularly buildings of a sensitive or prestigious nature. Identify any areas where an improvised explosive device could be hidden. If the configuration of the facility or area precludes implementation of this measure, take appropriate compensatory measures per local plans. Consider centralized parking.

- Measure 15—secure, seal, and regularly inspect all buildings, rooms, and storage areas that can be isolated with minimum site impact.
- Measure 16—at the beginning and end of each work day and at frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious activity or unattended packages and for signs of tampering or indications of unauthorized entry.
- Measure 17—implement screening procedures for all incoming official mail to identify possible explosive or incendiary devices or other dangerous material. If available, have explosive ordnance disposal (EOD)-trained teams inspect suspicious items and screen mail periodically. Provide guidance concerning suspicious packages. Encourage employees to inspect their individual mail, report suspicious items to security, and refrain from handling such items until cleared by the appropriate authority.
- Measure 18—inspect other deliveries and locally designated common-use facilities to identify explosives and incendiary, biological, or chemical devices. Use EOD-trained teams for some screening inspections when available. Instruct site personnel to report suspicious packages to security and refrain from handling them until cleared by the appropriate authority.
- Measure 19—increase both overt and covert security force surveillance of locally designated soft targets to improve deterrence and build confidence among site personnel.
- Measure 20—inform employees of the general threat situation. Limit visitors and escorted uncleared personnel. Periodically update all personnel as the situation changes to stop rumors and prevent unnecessary alarm.
- Measure 21—brief representatives of all activities on the site concerning the threat and security measures implemented in response to the threat. Explain reasons for actions. Implement procedures to provide periodic updates for these activity representatives.
- Measure 22—verify the identity of all personnel entering PPAs and other sensitive activities specified in local plans. Use of automated access control systems at interior security areas is acceptable and encouraged, where practical. Randomly, visually inspect the interior of all vehicles and the exterior of all suitcases, briefcases, packages, and other containers. Increase frequency of detailed vehicle inspections and the frequency of detailed inspections of suitcases, briefcases, and other containers.
- Measure 23—increase the frequency of random identity checks (inspection of security badges and vehicle registration documents) conducted by security force patrols on the site.
- Measure 24—remind all personnel to lock parked vehicles and inspect vehicles for suspicious items before entering and driving them.
- Measure 25—implement additional security measures for critical/sensitive personnel according to all existing plans.
- Measure 26—brief all security force personnel concerning the threat and policies governing rules of engagement, use of deadly force, and fresh pursuit. Ensure there is no misunderstanding of these instructions. Repeat this briefing on a periodic basis.

- Measure 27—increase liaison with local police, intelligence, security agencies, and the FBI to monitor the threat to site personnel and facilities. Notify local police agencies concerning SECON 2 or 1 measures that, if implemented, could affect their operations in the local community.
- Measure 28—survey the surrounding area to determine whether operational activities near the area might create emergencies or contingencies that could affect the site/facility.
- Measure 29—reserve for site/facility use.

SECON 2, High Condition (Orange). This condition is declared when there is a high risk of terrorist attacks. This condition applies when an incident occurs or intelligence is received indicating that some form of malevolent or terrorist action against personnel and facilities is imminent. Implementation of measures in this security condition for more than a short period probably will create hardship and affect the routine activities of the site and its personnel. For measures requiring an increase in the frequency of a specific action, the new frequency is to be more often than in the lower level SECON. The following measures should be implemented:

- Measure 30—continue all SECON 4 and SECON 3 measures or introduce those that have not already been implemented.
- Measure 31—recall staff representatives and initiate 24-hour operation of the EMT. Place the SRT on standby alert. Keep all personnel responsible for implementing special/response contingency plans at their places of duty. Review site evacuation plans.
- Measure 32—reduce site access points to the absolute minimum necessary for continued operation.
- Measure 33—verify the identity of all personnel entering the site/facilities, including appropriate offsite facilities under DOE control. Inspect all security badges for tampering. On a random basis, visually inspect the interior of all vehicles and the exterior of all suitcases, briefcases, and other containers. Increase the frequency of detailed vehicle inspections and the frequency of inspections of suitcases, briefcases, and other containers.
- Measure 34—implement centralized parking and shuttle bus service, where required.
- Measure 35—ensure that security personnel have been briefed concerning policies governing the rules of engagement, use of force, and fresh pursuit, particularly criteria for use of deadly force. Ensure that non-security supervisory personnel are familiar with above policies and procedures, if applicable. Ensure that special equipment and ammunition are available for immediate issue.
- Measure 36—increase security patrol activity to the maximum level sustainable. The concept of continuing random security patrol activity is encouraged.
- Measure 37—position security force personnel in the vicinity of critical facilities.
- Measure 38—erect barriers required to control direction of traffic flow and to protect facilities vulnerable to bomb attack by parked or moving vehicles.
- Measure 39—consult local authorities about closing public roads and facilities that might make sites more vulnerable to terrorist attacks.

- Measure 40—consider canceling public events.
- Measure 41—consider initiating continuity of operations plans.
- Measure 42—reserve for site/facility use.

SECON 1, Severe Condition (Red). This condition applies in the immediate area where a malevolent or terrorist attack has occurred that may affect the site or when an attack is initiated on the site. Implementing SECON 1 will create hardship and affect the activities of the site and its personnel. Normally, this SECON is declared as a localized response. For measures requiring an increase in the frequency of a specific action, the new frequency is to be more often than in the lower-level SECON. The following measures should be implemented.

- Measure 43—continue all previous SECON measures and introduce those that have not already been implemented.
- Measure 44—augment security forces to ensure absolute control over access to the site, facilities, and other potential target areas. Establish surveillance points; use night-vision devices.
- Measure 45—working closely with facility management, identify the owners of all vehicles already on the site. In those cases where the presence of a vehicle cannot be explained (owner is not present and the vehicle has no obvious site affiliation), inspect the vehicle for explosives; incendiary, chemical, or biological devices; or other dangerous items and remove the vehicle from the vicinity of facilities, soft targets, and other sensitive areas as soon as possible.
- Measure 46—inspect all vehicles entering the site. Inspections should include cargo storage areas, undercarriage, gloveboxes, and other areas where explosives, incendiary, chemical, or biological devices or other dangerous items could be concealed.
- Measure 47—limit access to the site, facilities and other areas to those personnel with a legitimate and verifiable need to enter. Implement positive identification of all personnel. No exceptions.
- Measure 48—inspect all baggage such as suitcases, packages, and briefcases brought on the site for explosives, incendiary, chemical, or biological devices, or other dangerous items.
- Measure 49—implement frequent inspections of the exterior of buildings (including roofs) and parking areas. Conduct inspections at facilities and in the vicinity of soft targets.
- Measure 50—coordinate with the operations division/center to establish communications, responsibilities, and authorities before, during, and after attack.
- Measure 51—request that local authorities close those public roads and facilities in the vicinity of the site/facilities that might facilitate execution of a malevolent or terrorist attack.
- Measure 52—cancel public events.
- Measure 53—execute continuity of operations plans.
- Measure 54—reserve for site/facility use.

3. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the objective and elements that are contained in a SSSP and SSP.

a. Discuss the application, scope, and purpose of a SSSP.

The following is taken from DOE M 470.4-1 chg 1.

Application

The SSSP is used to evaluate site and facility program elements and resources as they relate to identified threats and risks. The protection measures identified in approved SSSPs become the basis for executing and reviewing site protection programs.

Scope

The approved SSSP provides assurance that S&S measures address identified threats and risks. To provide this assurance, the plan must reiterate the assumptions identified to, and agreed upon, by line management. These assumptions must include reference to the contract under which the site is operated and those contractual issues that may impact S&S, applicable DOE directives, the threat upon which VAs are based, the methodology used to conduct VAs, deviations and proposed deviations, and any unique S&S impacting issues and assumptions that were addressed, and agreed to, by the responsible parties.

Purpose

The SSSP describes the graded protection of DOE assets required to be implemented by line management. The SSSP identifies site risks, cost-benefit analyses, and comparison of proposed upgrades. The resource plan (RP) must identify near- and long-term resource requirements needed to ensure the integrity of existing and planned S&S upgrades. The annual (at least every 12 months) review serves as the basis for tracking the implementation of protection measures and strategies necessary to maintain system effectiveness and identifies unfunded requirements.

b. Describe the following elements of a SSSP:

- **Site Description and Mission**
- **Site Threat Description and Target Identification**
- **Site Protection Strategies**
- **Physical Protection Systems**
- **Site PF**
- **Material Control and Accountability (MC&A) Program**
- **Site Personnel Security and Human Reliability Programs (HRP)**
- **Automated Information Security Program**
- **S&S Equipment Maintenance and Testing Programs**
- **Site Protection Evaluation Program**
- **Deviations from DOE Directives**
- **Summary of VA and Risk Assessment Results**

The following descriptions are taken from DOE M 470.4-1 chg 1.

Site Description and Mission

Site Mission Statement

Describe the site mission and how the mission relates to national security and the health and safety of the public, employees, and the environment. It describes the major programs or activities performed at the site in terms of mission and their relationship to the DOE national security mission.

Site Description and Area Layout

Describe the physical and geographical area in which the site and the S&S program are located. Provide a map, photograph, or drawing of the site that identifies locations of category I facilities, facilities with a credible roll-up of SNM to a category I quantity, the CAS and secondary alarm stations (SAS), security-related communications facilities, and other facilities of security interest. Show the location of barriers defining the site protected area (PA). A small-scale map or drawing should be used to show the relationship of the site to the surrounding area and be of sufficient detail to orient the user.

Site Threat Description and Target Identification

Threat Description

Establish a graded approach to protection for category I SNM and SNM facilities with credible roll-up of SNM to a category I quantity, and facilities having radiological, biological, or chemical, sabotage event potential and facilities having disruption of critical mission sabotage event potential. Use the DBT as the baseline for threat determination, along with higher levels of threat dictated by local and regional threats (when available), and describe the site-specific threats used as the basis for conducting VAs and for which the protection program is designed.

Target Identification

Identify, describe, and prioritize targets of security interest that meet the following criteria:

- Category I quantities of SNM and the facilities with credible rollup of SNM to a category I quantity.
- A radiological, biological, or chemical sabotage inventory that, if released, would cause an unacceptable impact on national security or the health and safety of employees, the public, or the environment.
- Critical national security facilities, and assets designated by the Department that would impact DOE programs supporting national defense and security.
- Those facilities possessing automated information systems that process or contain sensitive compartmented information (SCI), Special Access Program (SAP), weapon data classified Secret Restricted Data (S/RD) Sigma 1, 2, 14 and 15 or higher.

- Temporary recurring targets. When predictable programmatic operations can reasonably be expected to present temporary SNM, sabotage, or information targets such as those permanent locations previously described, these targets must be described and analyzed at the same level of detail and in the same manner as permanent locations.

Provide a brief introductory description of the targets and a chart or list that indicates the type of target, its location, attractiveness level, size, and configuration. Include SNM theft/diversion targets; radiological, biological, and chemical targets; and disruption of critical mission targets and those facilities possessing automated information systems that process SCI, SAP, weapon data classified S/RD Sigma 1, 2, 14, and 15 or higher.

Site Protection Strategies

Identify the protection strategies employed that address the overall protection program and enhance the concept of graded protection. Describe the protection program strategies employed. The basic strategies pertaining to protection are denial of access, denial of task, and containment that upon failure could evolve into recapture/recovery or pursuit strategies. Protection programs and tactical deployments designed to prevent unauthorized control of material and devices and to prevent acts of radiological, biological, chemical, and disruption of critical mission must be integrated with protection strategies. These activities could include protection layers of intrusion detection systems (IDS) and concentric security areas, access control measures, compartmentalization, insider protection programs, and procedural measures.

The plan should clearly convey the strategy to be employed, and plan reviewers will anticipate that procedures are available to ensure implementation of these strategies. Display in a chart, the protection strategy used, the facility and target involved, and the title and responsible office for each plan or procedure. Ensure the information provided is consistent with that found in DOE M 470.4-1 chg 1, chapter 2, *Site Threat Description and Target Identification*.

Physical Protection Systems

Describe the physical protection systems for each facility that has category I quantities of SNM; credible roll-up quantities of SNM to a category I quantity; radiological, biological, chemical and sabotage targets, and those facilities possessing automated information systems that process or contain SCI, SAP, weapon data classified S/RD Sigma 1, 2, 14 and 15, or higher. Provide a narrative description of the physical protection systems and how these systems are integrated at the site and facility level. Describe how physical protection systems are implemented to allow the PF to focus resources on its primary mission of defeating an armed terrorist threat. Describe how the barriers are protected by an IDS, security lighting, PF, and assessment systems and how structures located in or on the barrier are protected so as not to degrade protective systems. Describe the design of barrier systems used to deny vehicle approach routes to critical targets.

Site PF

Describe the PF organization and equipment deployed to perform 24-hour-per-day protection. Confirm that the basis for PF organization and planning is based on the identified site threat. Provide a narrative summary of the PF mission(s), capabilities, and deployment concepts used for site protection. Describe the methods used to review and prioritize post assignment priorities and eliminate posts that detract from combat readiness at high priority sites. Indicate the availability of plans and procedures that address normal and emergency deployment. Describe the PF equipment used including firearms, communications, vehicles, and any special items. Provide an organization chart of the PF, including response forces, showing the management and organization structure and key organizational interface positions with the cognizant security authorities and site operations and safety organizations. Using a schematic, display the PF communications network and include available secure networks and linkages to offsite law enforcement organizations with whom support agreements exist. In a chart, show the weapons and special equipment assigned to PF personnel, including members of the response force.

Material Control and Accountability (MC&A) Program

Describe the MC&A management program and summarize the results of the MC&A VA and other MC&A program planning activities. Describe the mission of the site MC&A organization. Summarize current and planned nuclear materials processing and storage activities. Using an organization chart, show the MC&A organization and management structure and the lines of authority and points of interface with other S&S programs, facility operations, and the cognizant security authorities' MC&A organizations. Describe the functions and responsibilities of safeguards personnel and indicate how MC&A activities are integrated with those of site protection programs and other facility organizations; include organizational responsibilities for those program elements that support multiple S&S programs (e.g., portal monitors and access controls). Confirm that MC&A personnel complete required training.

List, in a chart format, the facilities required to develop and maintain MC&A plans and procedures, the titles of those plans and procedures, and the office(s) responsible for approving and maintaining them.

Site Personnel Security and Human Reliability Programs

Describes the site-wide program for personnel security that, in conjunction with information and physical security programs, ensures only authorized access to classified information or matter, or SNM and confirms that the personnel security program is in conformance with and implements the requirements prescribed in current DOE policy. Describe the key elements of the site-wide personnel security program for access authorizations and, if applicable, the key element of the site's HRP. Describe the method(s) used at the site to ensure the appropriate level of access authorizations are issued for the category of material processed or stored at the site and for approving justification, processing, and reevaluating the need for such access authorizations. Indicate how the effectiveness of the program is assessed. Indicate the site procedures that require contractors to perform pre-hire checks to ensure proper qualifications

and suitability of the applicant before submitting requests for access authorizations. Briefly describe the programs used to mitigate the effectiveness of potential "insider" activities and the application of these programs in addressing insider concerns. Provide an organization chart showing the location of the personnel security organization in relationship to the CSA and other contractor S&S organizations. Provide an organization chart identifying the designated HRP management official in relationship to the CSA and the designated HRP certifying official. Verify that the site has a current HRP implementation plan. List, in chart format, the titles of site-wide personnel security-related plans and procedures, the HRP implementation plan, if applicable, and the office(s) responsible for implementing and maintaining them.

Automated Information Security Program

Briefly describe the automated information systems for those facilities possessing automated information systems that process SCI, SAP, weapon data classified S/RD Sigma 1, 2, 14, and 15 or higher. Provide an organization chart showing the responsible automated information systems security program and its relationship to the CSA and contractor organizations.

In a chart, list the title of the automated information systems security program plans and procedures with the associated office responsible for implementing and maintaining the plan and procedures, the plans and procedures governing the automated information system VAs with the associated office responsible for implementing and maintaining the plan and procedures, and the reports containing the results of the VAs.

S&S Equipment Maintenance and Testing Programs

Describe maintenance and testing programs and life-cycle planning, designed to enhance the continuous operability of S&S-related equipment used in the protection of category I SNM (including areas with credible roll up of SNM to a category I quantity), and classified automated information systems. Summarize in a narrative the maintenance and testing programs in use that ensure the availability and operability of S&S-related equipment and systems. Indicate the availability of compensatory measures/procedures that are used when equipment is taken out of service or otherwise not available. Describe how S&S maintenance and testing programs are incorporated into the performance assurance program plans. Indicate how the performance testing and other S&S site and facility maintenance programs comply with DOE policy. Describe the life-cycle planning conducted for major S&S equipment and component replacement. Relate how this planning is used to support and validate S&S equipment budget requirements.

In a chart, list the maintenance, testing, and records management programs; the relevant plans and procedures that implement the programs; and the responsible office, as these programs apply to equipment used by the PF, security-related systems, and equipment and instrumentation used by the PF, security-related systems, and equipment and instrumentation used for MC&A. Many of these may be addressed in a single maintenance and testing program. Describe the records management program used for scheduling, recording, and tracking identified S&S maintenance requirements, deficiencies, and testing schedules.

Site Protection Evaluation Program

In a narrative, describe the programs available and used to evaluate the effectiveness of S&S protection programs and the interaction of these evaluation tools (i.e., surveys may focus on shortfalls found in security inspections). Include in this narrative an outline of the PF tactical performance-testing program describing the evaluation mechanisms used by line management. At a minimum, the programs described in chapters 4, 5, 6, and 8 of the SSSP should be addressed and the evaluation plan or procedure identified. In a chart, list the names of the evaluation plans/procedures used by the CSA to assist in determining the effectiveness of site and facility protection programs and systems. List the office responsible for the evaluation plan/procedure and its purpose. Indicate, in a brief description, that performance testing is used to verify the effectiveness of S&S systems/programs and to validate VA activities. Briefly describe barriers and other systems that cannot be adequately performance-tested to demonstrate protection capabilities and their integration into protection strategies due to physical, operational, or policy parameters.

Deviations from DOE Directives

List all deviations that have been approved. In a table, list the deviation, the officially assigned deviation number, the directive reference, and the dates the deviation was approved and expires. Provide similar information for those deviations pending approval. This information should be displayed in a chart.

Summary of VA and Risk Assessment Results

Summarize the VA and risk assessments results for category I SNM; category II SNM; theft targets; radiological, biological, and chemical sabotage targets; and disruption of critical missions.

Confirm in the narrative that performance testing was used to validate VA input data and the results of the VA. Following the narrative, complete a matrix that identifies the risk associated with the results of the VA. Summarize the proposed corrective actions or upgrades in the matrix. For line item construction project work or other major capital expenditures, cite the source of the required funding. Use the RP information as the basis for this summary.

c. Discuss the application, scope, and purpose of a SSP.

The following is taken from DOE M 470.4-1 chg 1.

Application

The SSSP is used to evaluate site and facility program elements and resources as they relate to identified threats and risks. The protection measures identified in approved SSSPs become the basis for executing and reviewing site protection.

Scope

The approved SSSP provides assurance that S&S measures address identified threats and risks. To provide this assurance, the plan must reiterate the assumptions identified to, and

agreed upon, by line management. These assumptions must include reference to the contract under which the site is operated and those contractual issues that may impact S&S, applicable DOE directives, the threat upon which VAs are based, the methodology used to conduct VAs, deviations and proposed deviations, and any unique S&S impacting issues and assumptions that were addressed, and agreed to, by the responsible parties.

Purpose

The SSSP describes the graded protection of DOE assets required to be implemented by line management. The SSSP identifies site risks, cost-benefit analyses, and comparison of proposed upgrades. The RP must identify near- and long-term resource requirements needed to ensure the integrity of existing and planned S&S upgrades. The annual (at least every 12 months) review serves as the basis for tracking the implementation of protection measures and strategies necessary to maintain system effectiveness and identifies unfunded requirements.

d. Discuss the difference between the SSSP and the SSP.

The following is taken from DOE M 470.4-1 chg 1.

At locations where an SSSP is not required because of the limited scope of interests, an SSP must be developed to describe the protection program. SSPs must be approved by the local DOE CSA. Specialized plans must be developed to address protection programs for other protection operations. Requirements for specialized plans that may or may not be components of the SSP are set forth in the applicable DOE directives.

e. Discuss the plan review and approval process.

The following is taken from DOE M 470.4-1 chg 1.

The SSSP requires approval by DOE line management and concurrence by the cognizant head of the departmental element (see DOE M 470.4-1 chg 1, attachment 1). Such approval authority must be formally delegated to line management.

- Copies of approved SSSPs must be provided to the Office of Security for review and comment.
- Other security plans may be approved as stipulated in the applicable directive. If approving authority is not otherwise stipulated, these security plans may be approved by DOE line management.

The SSSP must be submitted to DOE line management within 150 days of the termination date of data collection and approved within 120 days of the submittal date. Directive changes, facility reconfiguration, a new VA, or other activities that occur after the stated effective date will not be considered for purposes of reviewing/approving the plan.

The SSSP must be reviewed annually (at least every 12 months). Updates to the SSSP that may significantly alter the agreed-upon protection philosophy or performance standards of

protection systems must be subjected to the formal VA process, and if changes are shown to significantly alter system effectiveness performance, the update(s) will be subject to the same concurrence and approval as stated in DOE M 470.4-1 chg 1, paragraph 3e(1).

An information copy of approved modifications must be provided to the Office of Security.

f. Discuss the application, scope, and purpose of a non-possessing security plan.

The following is taken from DOE M 470.4-1 chg 1

A contractor that will not possess classified information or matter, or SNM at the contractor's place of business and will only access such security activities at other cleared facilities must be cleared as a "non-possessing (NP) facility." An NP contractor must adhere to the security plans of the facilities where the contractor is afforded access to classified information or matter, or SNM. A separate security plan must be executed to cover the NP contractor's security responsibilities.

The following is taken from the *Security Plan for Non-Possessing Facilities*.

The purpose of the NP security plan is to prescribe requirements, restrictions, and other procedures necessary to perform on contracts to provide support services on U.S. government contracts requiring employees to obtain access authorizations ("Q" or "L" clearances). Under the terms of the contract(s), employees will work at other government facilities and require access authorizations (security clearances) to perform their assigned duties. The company will not be required to possess, store, discuss, or computer process classified materials within its corporate office areas.

4. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the objective and elements that are contained in a SSSP and SSP Resource Plan (RP).

a. Discuss the objective of the SSSP RP.

The following is taken from DOE M 470.4-1 chg 1.

The RP identifies S&S resources necessary to ensure protection of Department assets and identifies changes in resource requirements (i.e., operational requirements, capital equipment, general plant projects [GPPs], and line item construction project [LICP]) that directly impact risk, indirectly impact risk, or derive from changing S&S policy, directives, guidance, or other Department or departmental direction.

b. Describe the contents of the following RP elements:

- **Operational Requirements**
- **Capital Equipment**
- **General Plan Projects**

- **Line Item Construction Projects**
- **Unfunded/Unsupported Requirements**
- **Data to be included in the RP**

The following is taken from DOE M 470.4-1 chg 1.

Operational Requirements

Operational requirements must include, but are not limited to, material consolidation, facility mission changes, changes in the DBT impacting site operations, PF redeployments, maintenance and testing changes, PF manning levels, procuring technical expertise and support personnel, and additional training requirements. Summarize the pertinent information in a table such as outlined in DOE M 470.4-1 chg 1, table D-1, *Operational Requirements*. The table and supporting narrative must include

- the title of each operational requirement;
- the basis of the requirement (drivers behind the requirement);
- the funding profile and the impacts if not funded (if possible, state the impact in terms of probability of system effectiveness (P_E) and indicate if this is a new resource requirement);
- provide a status of operational requirements that were previously authorized but have not yet been completed; and
- provide a separate section for each operational requirement.

Capital Equipment

These procurements could include, but are not limited to, alarm and assessment system components, MC&A systems, access control system components, and equipment necessary to complete the S&S mission. Summarize the pertinent information in a table as outlined in DOE M 470.4-1 chg 1; table D-2, *Capital Equipment*. The table and supporting narrative must include

- a title for each capital equipment procurement;
- the basis of the requirement (drivers behind the requirement);
- the funding profile and the impacts if not funded (if possible, state the impact in terms of P_E and indicate if this is a new resource requirement);
- a status of capital equipment upgrades that were previously authorized but have not yet been completed; and
- provide a separate section for each capital equipment procurement.

General Plan Projects

These GPPs could include, but are not limited to, alarm and assessment systems/components, MC&A systems, access control systems/components, or infrastructure improvements. Summarize the pertinent information in a table as outlined in DOE M 470.4-1 chg 1; table D-3, *General Plan Projects*. The table and supporting narrative must include

- a title for each GPP;
- the basis of the requirement (drivers behind the requirement);

- the funding profile and the impacts if not funded (if possible, state the impact in terms of P_E and indicate if this is a new resource requirement):
- a status of general plan project upgrades that were previously authorized but have not yet been completed; and
- provide a separate section for each GPP.

Line Item Construction Projects

Summarize the pertinent information in a table as outlined in DOE M 470.4.1 chg 1; table D-4, *Line Item Construction Projects*. The table and supporting narrative must include

- a title for each LICP;
- the basis of the requirement (drivers behind the requirement);
- the funding profile and the impacts if not funded (if possible, state the impact in terms of P_E and indicate if this is a new resource requirement);
- the status of S&S upgrades that were authorized but have not yet been completed; discuss any changes to cost estimates identified in the previous RP; and
- provide a separate section for each LICP.

Unfunded/Unsupported Requirements

Summarize the pertinent information in a table such as outlined in DOE M 470.4-1 chg 1, table D-5, *Unfunded/Unsupported Requirements*. The table and supporting narrative must include

- a title for each unfunded requirement;
- the basis for the requirement (drivers behind the requirement);
- the type of resource requested;
- the fiscal year the requirement was originally identified;
- the proposed funding profile and impacts due to lack of funding (if possible, state the impact in terms of P_E); and
- provide a separate section for each unfunded requirement.

Data to be Included in the RP

Following are the types of data to be included in the RP:

- Basis
  - Compliance
  - Rick reduction
  - SSSP derived
  - Cost-efficiency
  - Operational efficiency
  - Enhanced operations
  - DBT change
- Type of expense
  - Operational=annual recurring cost that will need to be added to the budget baseline
  - Single=one time only expense paid from operating dollars

- Total costs
  - TEC[20]=Total estimated cost
  - TPC=Total project cost
- Resource type
  - OE=operational expense
  - CE=capital expense
  - GPP=general plant project
  - LICP=line item construction project
  - BASE FY=fiscal year in which the resources were identified and requested
- Impact
  - Continued risk
  - Cost escalation
  - Unable to comply with xxxx (list applicable directive)
  - Programmatic impact
  - Operational impact
  - Other (list)

5. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the objective and elements that are contained in the VA Program.

a. Describe the seven steps in conducting a VA.

The following is taken from DOE M 470.4-1 chg 1.

The seven steps in conducting a VA are:

- Assumptions—assumptions and scoping agreements must be defined. All assumptions must be documented in the VA report.
- Threat—the person responsible for the conduct of VAs, hereinafter referred to as the analyst, must understand how the DBT relates to VAs. The analyst performing the VA must apply DOE headquarters, regional, and local threat guidance.
  - DOE headquarters threat.
    - The DBT must be used to define the threat against which VA analysts evaluate the protection system.
    - The site's protective systems must be analyzed against the access control list (ACL).
  - Regional and local threats must be considered during the conduct of VAs.
- Targets—all security interests whose loss, theft, compromise, and/or unauthorized use will affect the national security and/or the health and safety of DOE and contractor employees, the public, the environment, or DOE programs are potential targets. The

analyst must consider target configurations and conditions, as well as operational conditions and acquisition times.

- Modeling—is used to analyze S&S programs, interests, assets, and the effectiveness of program implementation. Modeling can include computer-based tools and simulations, table-top analyses, and subject matter expert (SME) analyses. DOE M 470.4-1 chg 1, section E, appendix 3, *VA Modeling Tools*, lists those modeling tools approved by DOE. Methods to ensure that the models accurately reflect the facility posture must be part of the final VA results. The modeling process must establish critical pathways. The following must be considered:
  - facility characterization;
  - system effectiveness models and equations must be used;
  - response force times;
  - the probability of neutralization (P_N) must be calculated using data available regarding the PF response and their ability to interrupt and neutralize an adversary. The methods used must be documented and retained as part of the evidence file. The calculated number for P_N must be derived from more than one source, one of which must be joint tactical simulation (JTS), joint conflict and tactical simulation (JCATS), or FoF exercises;
  - blast-effect modeling must consider blast effects on barrier breaching, a force multiplier, and target buildings;
  - table-top methods used to determine system effectiveness must be documented and a means provided to allow for validation or verification;
  - radiological sabotage must be fully analyzed against the DBT and ACL. Existing information from safety analyses can be used but must be analyzed to consider deliberate rather than accidental release;
  - chemical and biological sabotage must be analyzed against the DBT and ACL;
  - the analysis must use the thresholds stated in DOE O 470.3A, *Design Basis Threat Policy*; and
  - the use of chemical and biological agents must be analyzed as a force multiplier. Methods of release and mitigation measures must be part of the analysis.
- Performance Testing—if conducted, the results of the following tests (including validation) must be considered in determining system effectiveness:
  - FoF exercises;
  - limited scope performance tests (LSPTs);
  - alarm response and assessment performance tests (ARAPTs);
  - breaching test data; and
  - critical system element tests.
- Results—the results of VAs indicate P_E. The VA results must be used for determining:
  - protection system effectiveness reporting;
  - S&S upgrades;
  - manning/armament levels for the PF; and
  - justifications for waivers of and exceptions to S&S policy.

- VA Practitioner Training—VA practitioners must successfully complete VA Program training within two years of appointment. This requirement can be met through the National Training Center (NTC).

b. Discuss the determination and reporting requirements of system effectiveness.

The following is taken from DOE M 470.4-1 chg 1.

"Figures of merit" is defined as numerical values and/or qualitative ratings assigned to component systems and personnel associated with the protection system. Collectively the qualitative and/or quantitative measures provide the basis for determining system effectiveness. Approved reference materials must be used to provide initial data and to calculate accurate detection and delay numbers. A list of approved references is provided in DOE M 470.4-1 chg 1. Reference materials are to be used only as a basis for the relative figures of merit. Non-default figures of merit must be documented and based on performance testing or engineering studies.

c. Describe the actions that must be taken for the following levels of security system effectiveness:
- **Low protection system effectiveness**
- **Marginal protection system effectiveness**

The following is taken from DOE M 470.4-1 chg 1.

Low Protection System Effectiveness
- Once a low protection system effectiveness condition that results in high risk is identified, that condition must be reported to the responsible departmental element within four hours.
- A corrective action plan must be submitted to the responsible departmental element within eight hours, with a copy to the Office of Security.

Marginal Protection System Effectiveness
- Once a marginal protection system effectiveness condition that results in moderate risk is identified, that condition must be reported to the responsible departmental element within two working days.
- A corrective action plan with recommendations must be submitted to the responsible departmental element within five working days with a copy to the Office of Security.

d. Describe the Vulnerability Assessment Certification Program for analyst responsible for the conduct of VAs.

The following is taken from DOE M 470.4-1 chg 1.

The analyst responsible for the conduct of VAs must complete the Department-approved training program (scheduled to be fully implemented by 2008).

The analyst must be certified as outlined in the *Vulnerability Assessment Certification Program Manual* which is currently under development. Any person currently conducting VAs may be "grandfathered" until such time as the *Vulnerability Assessment Certification Program Manual* is issued.

e. Describe the purpose and application of the VA modeling tools listed in Appendix 3—Vulnerability Assessment Modeling Tools of DOE M 470.4-1 Chg 1, *Safeguards and Security Program Planning and Management*.

The following is taken from DOE M 470.4-1 chg 1.

Modeling is used to analyze S&S programs, interests, assets, and the effectiveness of program implementation. DOE M 470.4-1 chg 1, section E, appendix 3, lists those modeling tools approved by the DOE.

f. Describe the purpose and application of the system performance effectiveness equation contained in Appendix 4—System Performance Effectiveness Equation of DOE M 470.4-1 Chg 1, *Safeguards and Security Program Planning and Management*.

The following is taken from DOE M 470.4-1 chg 1.

The methodology requires the determination of the probability of sensing, probability of assessment, and probability of detection at each layer. These are then combined to determine the contribution to overall system effectiveness represented by each layer. Mathematically, this can be expressed as the equation:

$$P_{EL} = P_{IL} \times P_{NL} = P_{DL} \times P_{NL} = P_{AL} \times P_{SL} \times P_{NL}$$

Where:

P_{EL} is the system effectiveness contribution for layer L;

P_{IL} – Probability of interruption given first detection at layer L, $P_{IL} = P_{DL}$ if detection on layer L is timely, and is equal to 0 ($P_{IL} = 0$) if detection is not timely;

P_{DL} – Probability of detection at layer L, $P_{DL} = P_{SL} \times P_{AL}$ on layer L. P_{DL} is the probability of first detection at layer L, given that detection has not occurred at an earlier layer, multiplied by the probability of sensing at an earlier layer, multiplied by the probability of sensing at layer L (P_{SL}) and the probability of assessment at layer L (P_{AL});

P_{SL} – Probability of sensing on layer L;

P_{AL} – Probability of assessment on layer L; and

P_{NL} – Probability of neutralization given first detection at layer L.

L is defined as the number of detection layers in the system before the critical detection point (CDP) in the adversary path(s). Detection after the CDP cannot not be counted.

P_E is defined as the system effectiveness of the layer. The system effectiveness of the layer is the product of the probability of interruption of the layer and the probability of neutralization given that detection occurred at that layer (P_I x P_N). The probability of neutralization is determined discretely for each layer given detection at the layer. The neutralization determination is made if detection (regardless of the extent) takes place at the layer in question. Neutralization will occur sometime past the detection point and would be valid for the probability of neutralization of that specific layer.

P_D of the layer is defined as the product of the probability of sensing and the probability of assessment of the layer (P_S x P_A). Note that detection and assessment will be different between the elements of the layer and between layers.

P_{IL} of the layer is defined as $P_{IL} = P_{DL}$ if detection on layer L is timely, and is equal to 0 (P_{IL}=0) if detection is not timely.

For those protection systems based on sensing, assessment, detection, interruption, and active neutralization of an adversary, credit can only be taken up to the "point on the pathway" at which the total of the adversary task time, engagement times, and delay times exceeds the PF response times. This limiting criterion eliminates credit being taken for protection system capabilities that are not engaged prior to the adversary completing their objective. For denial-based protection systems, the point on the pathway is the CDP. The CDP is defined as the point at which the protective force must have timely detection, assessment, and response to initiate a response to have a high probability of success in the neutralization of the adversary or denial of the adversary's task/objective. Therefore, for a facility employing multiple, complementary layers of protection, the representative total protection system effectiveness is calculated up to the point at which the protection systems can still effectively engage an adversary prior to completion of the objective.

The contributions of each layer along the adversary pathway are then combined to determine the overall system effectiveness, where the overall system effectiveness is provided by the sum of the contributions of each layer (only those encountered along the adversary pathway) to the system effectiveness.

An example of the system effectiveness equations for a three-layer system protecting SNM would be as follows:

In extended notation, the overall system effectiveness is:

$$P_E = (P_{A1} \times P_{S1} \times P_{N1}) + [(1 - (P_{A1} \times P_{S1})) \times (P_{A2} \times P_{S2} \times P_{N2})] + \{(1 - ((P_{A1} \times P_{S1}) + [(1 - (P_{A1} \times P_{S1})) \times (P_{A2} \times P_{S2})])) \times (P_{A3} \times P_{S3} \times P_{N3})\}$$

This reduces to:

$P_E = (P_{D1} \times P_{N1}) + [(1 - P_{D1}) \times (P_{D2} \times P_{N2})] + \{(1 - (P_{D1} + [(1 - P_{D1}) \times P_{D2}])) \times (P_{D3} \times P_{N3})\}$,

and since $P_{IL} = P_{DL}$ when detection is timely,

$P_E = (P_{I1} \times P_{N1}) + [(1 - P_{I1}) \times (P_{I2} \times P_{N2})] + \{(1 - (P_{I1} + [(1 - P_{I1}) \times P_{I2}])) \times (P_{I3} \times P_{N3})\}$

$P_E = P_{E1} + [(1 - P_{I1}) \times P_{E2}] + \{(1 - (P_{I1} + [(1 - P_{I1}) \times P_{I2}])) \times P_{E3})\}$

($P_{IL} = 0$) if detection is not timely

6. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the objective and elements that are contained in the Performance Assurance Program.

a. Discuss the following essential S&S protection elements validated by the Performance Assurance Program:
- **Operability and effectiveness**
- **Continuity**
- **Reliability**
- **Performance tests**
- **Documentation**

The following is taken from DOE M 470.4-1 chg 1.

Operability and Effectiveness

Programs must provide operability and effectiveness testing of each protection program essential element or component.

Operability tests provide measure of integrity and must check the essential elements or total system to confirm operability.

Performance tests provide comprehensive assurance that protection program elements are performing as designed and provide the required levels of protection.
- Performance tests results are used to validate the effectiveness of all elements of a layered S&S system.
- Performance tests are not substitutes for compliance with requirements.

Continuity

Performance assurance programs must evaluate operational continuity of all S&S essential elements. LSPTs and/or FoF tests may be used as a means of meeting specific performance assurance testing requirements. Performance assurance programs must be evaluated as part of the DOE survey and the facility self-assessment programs as described in DOE M 470.4-1 chg 1, section G.
- New protection program essential elements and components must be validated through acceptance testing before operational use.

- Essential elements that have been repaired or undergone maintenance must be validated through testing before use.
- The PF must be performance-tested, both individually and in small tactical units.
- Performance tests must ensure that approved protection strategies of denial, containment, recapture, recovery, and pursuit can be accomplished by the PF.
- Essential elements of the protection program security systems and subsystems are performance-tested to ensure that system detection, assessment, and response to alarms and adversarial actions meet stated requirements.

Reliability

Each essential element whose failure would reduce protection to an unacceptable level must be tested at frequencies that provide high assurance of operability and reliability.

- Testing frequencies must reflect site-specific conditions and operational needs.
- Testing frequencies must be documented for each essential element.

Performance Tests

At least every 365 days, an integrated performance test encompassing all essential protection elements associated with a comprehensive site or facility threat scenario must be conducted to evaluate the overall facility S&S effectiveness.

- Those category I facilities requiring denial protection strategies must conduct integrated performance testing on a quarterly basis (at least every 3 months).

OR

- Those sites with multiple category I facilities requiring denial protection strategies may rotate quarterly performance testing so that at least one facility is tested on a quarterly basis (at least every 3 months). However, an integrated performance test for all category I facilities must occur at least once every 365 days.

Documentation

Performance assurance program plan—must be an integral part of the SSSP/SSP, or MC&A plan as applicable. The performance assurance program plan must describe the program and its administration and implementation by

- identifying protection elements for the protection of category I and II SNM and Top Secret (TS) matter
- describing how the performance of these elements is to be ensured, including the manner in which credit is taken for activities performed by external oversight organizations
- addressing how deficiencies identified during performance assurance activities are to be corrected

Performance assurance reports—the results of performance assurance program testing must be documented.

Document retention—record-keeping systems must provide an audit trail for performance assurance activities and reports.

b. Describe the contents of the Performance Assurance Program.

The following is taken from DOE M 470.4-1 chg 1.

Performance assurance program plan—must be an integral part of the SSSP/SSP, or MC&A plan as applicable. The performance assurance program plan must describe the program and its administration and implementation by

- identifying protection elements for the protection of category I and II SNM and TS matter
- describing how the performance of these elements is to be ensured, including the manner in which credit is taken for activities performed by external oversight organizations
- addressing how deficiencies identified during performance assurance activities are to be corrected

7. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the objective and elements contained in the DOE Oversight Policy.

a. Discuss the purpose and general requirements of the DOE Oversight Policy.

The following is taken from DOE O 226.1A.

DOE O 226.1A, *Implementation of Department of Energy Oversight Policy*, provides direction for implementing DOE P 226.1A, *Department of Energy Oversight Policy*, which establishes DOE policy for assurance systems and processes established by DOE contractors and oversight programs performed by DOE line management and independent oversight organizations. The objective of DOE O 226.1A is to ensure that contractor assurance systems and DOE oversight programs are comprehensive and integrated for key aspects of operations essential to mission success.

DOE O 226.1A establishes the minimum requirements for implementing DOE P 226.1A. DOE O 226.1A does not preclude requirements in existing or new directives from being more rigorous for operations or activities where it has been determined that the risk or hazard necessitates more rigor.

Oversight and assurance processes may identify DOE directives or site-specific requirements that conflict, are unclear, or are incomplete. Deficiencies in DOE requirements will be brought to the attention of the responsible DOE HQ policy organization (the Office of Primary Interest) for resolution. Deficiencies in site-specific requirement will be brought to the attention of the contracting officer.

The four essential elements of an oversight program must be designed to work as a comprehensive system to provide assurance that DOE activities are safe and secure.

Oversight of high consequence activities, such as high hazard nuclear operations, require additional rigor, such as instituting central technical authorities (CTAs) for core nuclear safety functions. Documented oversight program plans and schedules must address the role of the CTAs and their support staff.

b. Discuss the four essential elements of the DOE Oversight Model.

The following is taken from DOE P 226.1A.

It is DOE policy to implement assurance systems and oversight programs that include four essential elements:

- A comprehensive and rigorous assurance system is implemented at all sites.
- DOE field element line management oversight processes, such as inspections, reviews, surveillances, surveys, operational awareness, and walkthroughs that evaluate programs and management systems and the validity of the site assurance system.
- DOE Headquarters line management oversight processes are focused primarily on the DOE field elements. To the extent necessary, DOE headquarters line management also looks at contractor activities to evaluate the implementation and effectiveness of field element line management oversight.
- Independent oversight processes are performed by DOE organizations that do not have line management responsibility for the management of the activity and thus provide an independent perspective for senior management on the effectiveness of programs and activities at all organizational levels (headquarters, field, and contractor).

c. Describe the following security assurance activities:

- **Assessments (including self-assessments or management assessments, operational awareness or management walk-throughs, quality assurance assessments, and internal independent assessments).**
- **Event reporting (including reporting, analyzing, and trending operational events).**
- **Worker feedback mechanisms.**
- **Issues management (including analysis of causes; identification of corrective actions; corrective action tracking, monitoring and closure; verification of effectiveness; trend analysis; and identification of continuous improvement opportunities).**
- **Lessons learned.**

Assessments

The following is taken from DOE O 226.1A.

A rigorous and credible assessment program is the cornerstone of effective, efficient management of programs such as environment, safety, and health (ES&H); S&S; cyber security (CS); and emergency management (EM).

Self-assessments are used to evaluate performance at all levels periodically and to determine the effectiveness of policies, requirements, and standards and the implementation status.

- Management self-assessments are performed by contractor management, and are developed based on the nature of the facility/activity being assessed and the hazards and risks to be controlled.
- Self-assessments focus on hands-on work and the implementation of administrative processes, involve workers, supervisors, and managers to encourage identification and resolution of deficiencies at the lowest level practicable.
- Support organizations will perform self-assessments of their performance and the adequacy of their processes.
- Contractors, at all levels, will assess the implementation and adequacy of their processes, including analysis of the collective results of lower-level self-assessments.
- Self-assessment results will be documented commensurate with the significance of and risks associated with activities being evaluated. Deficiencies will be accurately described and documented for evaluation and correction using formal issues management processes.

Internal independent assessments will be performed by contractor organizations or personnel that have authority and independence from line management, to support unbiased evaluations.

- The assessments will be formally planned and scheduled based on the risk, hazards, and the complexity of the processes and activities to be evaluated.
- Independent evaluators will be appropriately trained and qualified and have knowledge of the areas assessed.
- Reviewers will be dedicated contractor staff, members of external organizations, or both.
- Although independent assessments are applied to individual activities and processes, they will typically focus on entire facilities or projects, and programs and management processes that are used by multiple organizations.
- Internal independent assessments will concentrate on performance and observation of work activities and the results of process implementation.

Event Reporting

The following is taken from DOE O 226.1A.

Formal programs will be established and effectively implemented to identify issues and report, analyze, and address operational events, accidents, and injuries.

- Reportable occurrences that meet occurrence reporting and processing system thresholds and associated corrective actions will be evaluated, documented, and

reported as required by DOE M 231.1-1A chg 2, *Environment, Safety and Health Reporting Manual*.

- For activities covered by the Price-Anderson Amendments Act, nuclear and worker safety and health issues meeting DOE reporting thresholds should be self-reported through the DOE-wide noncompliance tracking system to mitigate the severity level of the violation and potential financial penalties.
- Trending analysis of events, accidents and injuries is performed according to structured/formal processes.

Worker Feedback

The following is taken from DOE O 226.1A.

In addition to structured assessments, DOE contractors will establish and implement processes to solicit feedback from workers and work activities. Common feedback mechanisms are described in site plans/program documents and include the following:

- Employee concerns programs
- Telephone or internet "hotline" processes for reporting concerns or questions
- Pre-job briefs
- Job hazard walk-downs by workers prior to work
- Post-job reviews
- Employee suggestion forms
- Safety meetings
- Employee participation in committees and working groups
- Labor organization input

Issues Management

The following is taken from DOE O 226.1A.

Contractors must ensure that a comprehensive, structured issues management system is in place. This system must provide for the timely and effective resolution of deficiencies, and be an integral part of effective contractor assurance system.

Program and performance deficiencies, regardless of their source, must be captured in a system or systems that provide for effective analysis, resolution, and tracking. Issues management must include structured processes for

- determining the risk, significance, and priority of deficiencies
- evaluating the scope and extent of the condition or deficiency
- determining event reportability under applicable requirements
- identifying root causes
- identifying and documenting suitable corrective actions and recurrence controls, based on analyses, to correct the conditions and prevent recurrence
- identifying individuals/organizations responsible for implementing corrective actions
- establishing appropriate milestones for completion of corrective actions, including consideration of significance and risk

- tracking progress toward milestones such that responsible individuals and managers can ensure timely completion of actions and resolution of issues
- verifying that corrective actions are complete
- validating that corrective actions are effectively implemented and accomplish their intended purposes, using a graded approach based on risk
- ensuring that individuals and organizations are accountable for performing their assigned responsibilities

Issues management will provide a process for rapidly determining the impact of identified weaknesses and taking timely action to address conditions of immediate concern. For such conditions, interim corrective actions are to be taken as soon as a condition is identified and without waiting until a formal report is issued.

Processes for analyzing deficiencies, individually and collectively, must be established to enable the identification of programmatic or systemic issues. Process products will be used by management to monitor progress in addressing known systemic issues and to optimize the allocation of assessment resources.

Sites must have effective processes for communicating issues up the management chain to senior management, using a graded approach that considers hazards and risks. The processes must provide sufficient technical basis to allow managers to make informed decisions and must include provisions for communicating and documenting dissenting opinions. Processes for resolving disputes about oversight findings and other significant issues must be implemented. The processes must include provisions for independent technical reviews of significant issues.

Lessons Learned

The following is taken from DOE O 226.1A.

Formal programs must be established to communicate lessons learned during work activities, process reviews, and event analyses to potential users and applied to future work activities. Contractors must identify, apply, and exchange lessons learned with the rest of the DOE complex. Contractors must review and apply lessons learned identified by other DOE organizations and external sources to prevent similar occurrences.

d. Discuss the activities conducted in contractor S&S oversight assessments.

The following is taken from DOE O 470.2B.

The Office of Independent Oversight and Performance Assurance (OA) has the responsibility for independent oversight within DOE, reporting directly to the Secretary. To provide an objective evaluation of the Department's performance, OA is independent of all other DOE elements that have line, program management, and/or policy development responsibilities for S&S; CS; EM; or ES&H programs.

Basis for Independent Oversight and Performance Assurance Activities. OA is the DOE focal point for independent evaluation of DOE sites, facilities, organizations, and operations in the areas of S&S; CS; EM; and ES&H.

The following are to be used as the basis for independent oversight: DOE Orders, notices and manuals; approved site S&S plans, CS plans, and other security plans; DOE threat statements; emergency management program plans; approved site safety management system description documents, integrated safety management (ISM) contract clauses, other ISM implementation documents, and other quality assurance documentation; safety basis, authorization basis, and authorization agreements; applicable statutes and rules; other contractually mandated requirements; and approved deviations. Other DOE guidance, while not to be considered or applied as requirements, may be used to augment and strengthen the baseline by providing supplemental information about acceptable methods for implementing requirements contained in Orders, notices, and manuals.

OA evaluates the effectiveness of line management performance in S&S; CS; EM; and ES&H programs to determine the adequacy of DOE policy and policy implementation.

Licensed DOE Facilities or Activities. Independent oversight activities for DOE facilities or activities licensed by the NRC must, except where excluded by law or DOE policy, be structured to minimize or eliminate duplication of oversight efforts while ensuring DOE security interests; EM; and ES&H programs and associated facilities are independently evaluated. Accordingly, the scheduling of independent oversight activities must take into account the inspection and assessment activities of the NRC.

8. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the objectives and elements that are contained in the surveys, reviews, and self-assessments conducted by different levels of DOE management, and demonstrate the ability to conduct surveys, reviews, and self-assessments.

a. Discuss the objectives of the survey, review, and self-assessment programs.

The following is taken from DOE M 470.4-1 chg 1.

The objectives of the survey, review, and self-assessment programs are:

- Provide assurance to the Secretary of Energy, departmental elements, and other government agencies (OGAs) that S&S interests and activities are protected at the required levels.
- Provide a basis for line management to make decisions regarding S&S program implementation activities, including allocation of resources, acceptance of risk, and mitigation of vulnerabilities. The results must provide a compliance- and performance-based documented evaluation of the S&S program.

- Identify S&S program strengths and weaknesses, develop and complete a process improvement schedule, and use the results to correct and improve the overall S&S program.
- Provide documentation of oversight and assessment activities.

b. Discuss the various types and frequencies of the following surveys and assessments:
- **Initial surveys**
- **Periodic surveys**
- **Special surveys**
- **Termination surveys**
- **Periodic reviews**
- **Self-assessments**
- **Reviews or inspections by other DOE elements or Other Government Agencies (OGA)**
- **Extension of frequency**

The following is taken from DOE M 470.4-1 chg 1.

Initial Surveys

Initial surveys must be conducted at facilities where there will be a facility clearance (FCL) established for a facility with an importance rating of: A, B, C, or Property Protection (PP). Survey activities must be comprehensive and result in a satisfactory composite rating prior to an FCL being granted.

Periodic Surveys

Periodic surveys are conducted for all facilities and must cover all applicable topics to ensure survey program objectives are met. The periodic survey may be composed of multiple special survey reports, providing all the requirements of this section are met. Integration of internal and external reports including quality assurance, property appraisals, performance assurance, and other evaluation reports may be used to augment the requirement for a periodic survey. A DOE Federal facility conducting a periodic survey fulfills the self-assessment requirement as noted in DOE M 470.4-1 chg 1, section G, paragraph 2a(6).
- Facilities with importance ratings of A, B, or C must be surveyed once every 12 months (with the exception of category IV SNM only facilities).
- Facilities with an importance rating of PP must be surveyed once every 24 months.
- Facilities with category IV SNM and nuclear material, including source material, the nuclear MC&A topical area must be surveyed at least every 24 months.
- Facilities with importance ratings of D, NP, or Excluded Parent (E) do not require surveys but do require periodic reviews.

(Note: Ratings explained in DOE M 470.4-1 chg 1, chapter II.)

Special Surveys

Special surveys may be conducted at facilities for specific limited purposes. Examples include extended survey activities, technical security activities, “for cause” reviews, line

management direction, shipment of nuclear and/or classified information or matter, or a change in the contractor operating a government-owned facility.

Termination Surveys

Termination surveys must be conducted to verify the termination of departmental activities and appropriate disposition of S&S interests. Examples of survey activities include: the appropriate disposition, destruction, or return of classified information or matter, SNM, hazardous material, and property; security badge retrieval; debriefings; and verification of the termination or transfer of DOE access authorizations. Onsite termination surveys must be conducted at facilities possessing TS matter, SCI/SAP information or matter, or SNM. Onsite or correspondence termination surveys must be accomplished for all other possessing facilities.

Periodic Reviews

A documented review of entities (D, NP, and E facilities) such as subcontractors, consultants, and common carriers must be performed by the DOE CSA at least every five years.

Self-Assessments

Self-assessments must be conducted between the periodic surveys conducted by the CSA and include all applicable facility S&S program elements. The self-assessment must ensure the S&S objectives are met. Federal facilities may use the self-assessment to substitute for the periodic survey requirement. NP facilities are not required to conduct self-assessments. However, sponsoring organizations (Federal or contractor) must include in their self-assessments a thorough review of their registration program for NP facilities which may result in a program review of identified subcontractors.

Reviews or Inspections by Other DOE Elements or OGA

Reviews/inspections conducted by other DOE elements (including site quality assurance programs) or OGAs may be used to meet survey requirements. When using reviews/inspections conducted by other organizations to meet the requirements of the survey, the guidelines below must be followed:

- The review/inspection must have been conducted within the survey period.
- Applicable portions of the review/inspection must be attached to the survey report.
- Portions of topical and subtopical areas not covered by the review/inspection must be surveyed.
- If ratings were not assigned during the review/inspection, the surveying office must analyze the impact of any deficiencies and assign ratings.

Extension of Frequency

The results of previous surveys may affect the frequency of future surveys. The interval between periodic surveys may be increased up to 24 months by the DOE CSA. Documentation of the justification for increases in the interval of periodic surveys must be maintained by the DOE CSA.

- The following conditions must be met for extensions:

- The facility was rated satisfactory during the most recent survey activity.
- The facility has no unmitigated deficiencies that impact the security posture of the facility, and all applicable topical area ratings are satisfactory from the previous survey.
- All applicable topical area ratings from the most recent self-assessment are satisfactory, and the DOE CSA concurs with the ratings.

- Increasing the interval between surveys for a facility possessing category I SNM or with credible roll-up to category I SNM must be approved, in writing, by the Associate Administrator for Defense Nuclear Security or the Under Secretary for Energy, Science, and Environment.
- All modifications to survey frequency requirements must be documented in the safeguards and security information management system (SSIMS).

c. Discuss the following activities and the methods that must be included in surveys and assessments:
- **Compliance**
- **Performance**
- **Comprehensiveness**
- **Determinations of survey scope predicated on the nature or status of operations at the facility, activity, or element being surveyed**

The following is taken from DOE M 470.4-1 chg 1.

Surveys and self-assessments must provide an integrated evaluation of all topical and subtopical areas to determine the overall status of the S&S program and ensure the objectives of DOE M 470.4-1 chg 1, section G, paragraph 1, are met. The integrated evaluation is a comprehensive synergistic approach using multiple S&S program elements that ensures total system effectiveness and, if properly implemented, will meet the objectives identified in DOE M 470.4-1 chg 1, section G, paragraph 1. The scope of these activities and the methods used must include:

- Compliance—reflects the status of the S&S program as measured against implementation of applicable Federal statutes, regulations, policies, approved SSSPs/SSPs, and other approved security plans.
- Performance—indicates the degree to which the elements of the S&S program meet protection objectives based on the operational testing of program elements.
- Comprehensiveness—identifies the breadth of protection afforded all activities and interests within a facility. This is accomplished by an evaluation of the adequacy and effectiveness of programs and a thorough examination of the implementation of policies, practices, and procedures to ensure compliance and performance. All applicable topical areas identified on DOE Form (F) 470.8, *Survey/Inspection Report*, must be evaluated.
- Other—The scope of special and termination surveys is determined by the DOE CSA in coordination with the surveying office. Determinations of survey scope are predicated on the nature or status of operations at the facility, activity, or element

being surveyed. These surveys may not cover all topical areas identified on DOE F 470.8.

d. Discuss the survey or self-assessment procedures that must be developed, documented, approved by the Cognizant Security Authority (CSA), and performed including the following:
- **Team composition**
- **Planning, scheduling, and integration**
- **Validation**
- **Exit briefing**

The following is taken from DOE M 470.4-1 chg 1.

Local survey and self-assessment procedures implementing DOE M 470.4-1 chg 1, section G, must be developed, documented, and approved by the CSA. Procedures must ensure completion of the objectives contained in DOE M 470.4-1 chg 1, section G, paragraph 1, and must include the requirements listed below.

- Team composition—survey and self-assessment team personnel must possess qualifications, experience, and training sufficient to review and inspect the topical/subtopical areas of the survey/self-assessment. The NTC provides training courses for survey team leaders and team members.
  - Survey teams must be led by a Federal employee and may be composed of departmental Federal contractor personnel.
  - Self-assessments must include at least one person from the CSA.
- Planning, scheduling, and integration—surveys and self-assessments must be planned, scheduled, and conducted in an integrated manner to achieve the objectives identified in DOE M 470.4-1 chg 1, section G, paragraph 1. If topical and subtopical area evaluations are performed separately, the surveying office must document and integrate the results of each into a single (periodic) survey report that includes a composite facility rating. The frequency between topical and subtopical areas cannot exceed the frequency for the single (periodic) survey.
- Validation—results must be validated by methods including, but not limited to, document reviews, performance testing, and interview analyses and observation.
- Exit briefing—must be conducted with the surveyed or assessed organization to include the minimum facts:
  - Program strengths and weaknesses, including all findings.
  - Corrective action reporting requirements for all open findings, regardless of source.
  - Topical and composite ratings. For less than satisfactory ratings, the communication of the composite rating initiates the actions required in DOE M 470.4-1 chg 1, section G, paragraph 8.

e. Discuss the definition of the term "findings" as it relates to surveys, reviews, or self-assessment programs.

The following is taken from DOE M 470.4-1 chg 1.

Findings are any validated program deficiency (failure to meet a performance or compliance requirement) regardless of source. Findings may be reflected in documents resulting from internal and external reviews, audits, appraisals, and other sources.

All open findings must be reviewed during the survey or self-assessment to validate the status of corrective action and to evaluate the impact on the existing S&S program.

Findings identified during the current survey or self-assessment must be reported immediately to the departmental element and contractor line management if a vulnerability to national security, classified information or matter, nuclear materials, or Department property results, or may result, in a programmatic impact to the Department. Findings identified during a survey or self-assessment, even if closed during the survey or self-assessment activity must be documented in the associated report.

f. Discuss the requirements for the administration of the identified finding.

The following is taken from DOE M 470.4-1 chg 1.

Findings and deficiencies, regardless of source, and corrective action plans (milestones and estimated completion dates) must be entered into SSIMS according to SSIMS guidelines and tracked until closed. Quarterly status reports must be entered into SSIMS by January 15, April 15, July 15, and October 15 of each year. Self-assessment deficiencies are not required to be entered into SSIMS; however, a local mechanism/system must be used to track these deficiencies and corrective action until closed.

Trending evaluations must be considered in the resolution of findings in the subtopical area of program management to determine if systemic and systematic causal factors exist within the S&S program. Results of this evaluation that indicate negative trends must be analyzed to ensure corrective action plans address root causes and the need to ensure continuous improvement of the S&S program.

g. Discuss the following types of ratings that must be used for all surveys (except termination), reviews, and self-assessments:

- **Satisfactory**
- **Marginal**
- **Unsatisfactory**
- **Inspection Ratings**
- **Does Not Apply (DNA)**
- **Not Rated (NR)**

The following is taken from DOE M 470.4-1 chg 1.

Ratings must be based on the effectiveness and adequacy of the program at a facility and reflect a balance of performance and compliance results as well as the impact of the deficiency(ies) (e.g., findings, Office of Inspector General (IG) recommendations, etc.) and mitigating factors. The ratings listed below must be used for all surveys (except termination), reviews, and self-assessments. DNA and NR may also be used in applicable situations.

Types of ratings:

- Satisfactory—the element being evaluated meets protection objectives or provides reasonable assurance that protection objectives are being met.
- Marginal—the element being evaluated partially meets protection objectives or provides questionable assurance that protection objectives are being met.
- Unsatisfactory—the element being evaluated does not meet protection objectives or does not provide adequate assurance that protection objectives are being met.
- Inspection Ratings—"Effective Performance," "Needs Improvement," and "Significant Weaknesses" are indicators of a management system performance level as outlined in DOE O 470.2B, *Independent Oversight and Performance Assurance Programs*.

h. Discuss the factors used to determine the assigned ratings.

The following is taken from DOE M 470.4-1 chg 1.

Rating determinations.

- Existing conditions—ratings must be based on existing conditions at the end of the survey and not future or planned corrective actions or conditions.
- Impact—ratings must be based on the impact of all open deficiencies, regardless of source.
- Marginal or Unsatisfactory ratings—less than satisfactory ratings in any topical area must be based on validated weaknesses in the S&S system or deficiencies in performance.
- Topical area ratings—a topical area rating must not be marginal for consecutive survey periods and must be assigned an unsatisfactory rating unless one of the following conditions applies:
  - The current survey of the topical area results in a satisfactory rating.
  - The previous survey that resulted in a marginal rating identified different deficiencies and reasons for the rating.
  - The deficiencies and reasons that were the basis for the previous marginal rating were related to the completion of an LICP or upgrade program. In that case, acceptable interim measures must have been implemented, physically validated pending completion of the project, and documented in the survey report.
- Subtopical ratings—the decision whether or not to use all subtopical ratings must be documented in local procedures. Regardless of the rating method used, the report must include the evaluation of all required subtopical areas which must be used as part of the appropriate topical area rating justification and rationale.

- Justification and rationale—all ratings must be supported and documented to include the rating justification and rationale.

i. Discuss the items that must be contained in the following reports:
- **Initial/periodic survey and self-assessment**
- **Special survey**
- **Non-possessing facilities**
- **Termination survey**
- **Memorandum**

The following is taken from DOE M 470.4-1 chg 1.

Initial/Periodic survey reports and self-assessment reports must contain the following:
- A completed DOE F 470.8 (or equivalent for self-assessments)
- An executive summary containing
  - the scope, methodology, period of coverage, duration, date of the exit briefing to management;
  - a brief overview of the facility, function, scope of operations, and contractual information (e.g., contract number, award and expiration dates, contract type, identification of security clauses, identification of the security, and overall scores assigned to the most recent contract appraisal);
  - a brief synopsis of major strengths and weaknesses that impact the effectiveness of the facility's overall S&S program, including identification of any topical areas rated less than satisfactory;
  - the overall composite facility rating with supporting rationale; and
  - a reference to a list of findings identified during the survey or self-assessment.
- An introduction containing
  - the scope, methodology, period of coverage, duration, and date of the exit briefing to management; and
  - a description of the facility, its function and scope of operations, security interests, and contractual information.
- Narrative for all rated topical and subtopical areas that includes
  - a description of the site's implementation of the program element;
  - the scope of the evaluation;
  - a description of activities conducted;
  - the evaluation results and associated issues (including other department elements or OGA review or inspection results related to this topic/subtopic that were included in the survey);
  - the identification of all findings, including new and previously identified open findings, regardless of source and their current corrective action status; and
  - an analysis that provides a justification and rationale of the factors responsible for the rating.
- Attachments, including

- a copy of the current DOE F 470.2, "Facility Data and Approval Record" (FDAR);
- a listing of all active DOE F 470.1, "Contract Security Classification Specification" (CSCS), or DD F 254, "Contract Security Classification Specification";
- a listing of all new findings resulting from the survey/self-assessment;
- a listing of all previous findings that are open, to include the current status of corrective action;
- a listing of team members including names, employer, and their assigned area(s) of evaluation; and
- a listing of all source documentation used to support the survey/self-assessment conduct and results.

Special survey reports—must follow the format and content for initial and periodic survey/self-assessment reports except that an executive summary is not required. Attachments must be included as appropriate to the scope of the special survey.

Reports for NP facilities must include

- a completed DOE F 470.8, "Survey/Inspection";
- a copy of the DOE F 470.2 FDAR;
- a list of each active DOE F 470.1 CSCS or DD F 254;
- an evaluation of the foreign ownership, control, or influence (FOCI) status;
- a determination that employees and subcontractors possess appropriate access authorizations;
- a review to ensure that individuals no longer employed on the contract have had their access authorizations terminated and security badges have been accounted for; and
- other topical/subtopical areas identified on DOE F 470.8 as required by the DOE CSA.

Termination survey reports must include

- verification of non-possession of classified information or matter, SNM, hazardous material presenting a potential sabotage threat, or government property;
- verification that all DOE access authorizations have been terminated or transferred and that termination statements have been completed and security badges have been accounted for;
- validation that all findings have been closed in SSIMS;
- verification of termination of all S&S activities;
- a copy of the terminating DOE F 470.2 FDAR; and
- a completed certificate of non-possession.

Memorandum reports for DOE programmatic entities and OGAs are generated when it is inappropriate to transmit a copy of the survey report due to need-to-know issues. Reports must contain

- a notification of inclusion of their activity in the survey
- the date of the survey

- ratings and rationale for the ratings associated with the activity
- all findings applicable to that activity

j. Conduct a survey, review, or self-assessment.

This is a performance-based KSA. The Qualifying Official will evaluate its completion.

9. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the Foreign Ownership, Control, or Influence (FOCI) Program requirements and criteria to facilitate the initial and continued Facility Clearance (FCL) eligibility of U.S. companies with/or without foreign involvement.

a. Discuss the objectives of the FOCI Program.

The following is taken from DOE M 470.4-1 chg 1.

The objective of the FOCI Program is to establish the FOCI Program requirements and criteria to facilitate the initial and continued FCL eligibility of U.S. companies with foreign involvement.

b. Discuss the entities required to obtain FOCI determinations.

The following is taken from DOE M 470.4-1 chg 1.

The entities listed below are required to obtain FOCI determinations:

- Applicants, including industrial; educational; commercial; or any other entity, grantee, or licensee, including an individual, that have or anticipate executing a classified contract. This includes subcontractors of any tier, consulting firms, agents, grantees, and cooperative research and development agreement participants who require access authorizations.
- All tier parents located in the United States, Puerto Rico, or a U.S. possession or trust territory.

c. Discuss the DOE Acquisition Regulation (DEAR) restrictions on awarding of classified contracts prior to the issuance of a FCL.

The following is taken from DOE M 470.4-1 chg 1.

The DEAR prohibits the award of a classified contract until an FCL has been granted. When an existing contract that does not require access authorizations is modified to require access authorizations, the contract modification cannot take effect until an FCL is granted. Contract award/modification cannot be made until

- all relevant aspects of FOCI have been resolved and, if necessary, are favorably adjudicated;
- the signed DOE F 470.1, "CSCS" is accepted by the CSA; and

- the appropriate DEAR security clauses have been incorporated in the contract.

d. Describe the procedures for using the Department's electronic system for applicants to submit FOCI information to DOE in an electronic format.

The following is taken from DOE M 470.4-1 chg 1.

The Department has an electronic system for applicants to submit FOCI information to DOE in an electronic format. To ensure confidentiality of the information submitted and stored on the system, the site is protected with 128-bit encryption.

- Applicants may use this system for the submission of FOCI packages, including changes to update their FOCI information. The FOCI web site may be accessed via an Internet browser at https://foci.td.anl.gov. Electronic signatures are not accepted; therefore, a signed original Standard Form (SF) 328, "Certificate Pertaining to Foreign Interests," executed according to the instructions on the certification section of the SF 328, must be submitted to the DOE CSA.
- Federal employees and supporting contractors should use the electronic submission processing system website at http://greylist.td.anl.gov.

10. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the policies and procedures for FCLs and registration of S&S activities.

a. Discuss the eligibility requirements of the FCL program.

The following is taken from DOE M 470.4-1 chg 1.

The following delineates the primary requirements of the FCL program.

- A contractor requiring an FCL must be sponsored by
  - a government contracting activity (i.e., a contracting officer); or
  - a cleared contractor acting as the prime contractor for the uncleared contractor. Contractors cannot sponsor themselves for an FCL.
- The contractor or prospective contractor must meet the following eligibility requirements prior to being processed for an FCL. The contractor or prospective contractor must
  - need an FCL in connection with a legitimate U.S. government or foreign requirement;
  - be organized under the laws of one of the 50 states, the District of Columbia, or Puerto Rico and must be located in the U.S. or a U.S. territorial area or possession;
  - have a reputation for integrity and lawful conduct in its business dealings;
  - not have been barred from participating in U.S. government contracts. This includes key management personnel (KMP) on the contract; and
  - not be under FOCI to a degree that the granting or continuation of the FCL would be inconsistent with common defense and national security. This requirement

only applies when the contract awarded or to be awarded requires access authorizations.

b. Discuss the activities that occur on premises occupied by the Department or its contractors that require an FCL.

The following is taken from DOE M 470.4-1 chg 1.

An FCL must be granted before any nuclear or other hazardous materials presenting a potential radiological, chemical, or biological sabotage threat; classified information or matter; or PP interests are placed on premises occupied by the Department or its contractors.

c. List the company officials that must be granted access authorizations in order for the company to qualify for an FCL involving classified information or matter, or SNM.

The following is taken from DOE M 470.4-1 chg 1.

Certain company officials must be granted access authorizations in order for a company to qualify for an FCL involving classified information or matter, or SNM. These company officials include the owners, officers, directors, partners, regents, trustees, or executive personnel (i.e., those considered KMP).

d. Define the term "non-possessing facility."

The following is taken from DOE M 470.4-1 chg 1.

A contractor that will not possess classified information or matter, or SNM at the contractor's place of business and will only access such security activities at other cleared facilities must be cleared as an NP facility." An NP contractor must adhere to the security plans of the facilities where the contractor is afforded access to classified information or matter, or SNM. In addition, a separate security plan must be executed to cover the NP contractor's security responsibilities.

11. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the S&S Training Program.

a. Discuss the objectives of the S&S Training Program.

The following is taken from DOE M 470.4-1 chg 1.

The objective of the S&S training program is to establish programs that ensure personnel are trained to a level of proficiency and competence that ensures they are qualified to perform assigned S&S tasks and/or responsibilities.

b. Discuss the following requirements of the S&S Training Program:

- **Key program elements**
- **Job analysis**
- **Testing**
- **Training content**
- **Training course development**
- **Training Approval Program (TAP)**
- **Training records management**
- **Training plans**

The following is taken from DOE M 470.4-1 chg 1.

Key Program Elements

The S&S training program must encompass the following key S&S program elements:

- Program planning and management
- Personnel security
- Physical protection
- Protective force
- Nuclear MC&A
- Information security

Job Analysis

A job analysis must identify, describe, and document major task and skill requirements.

Testing

Knowledge- and/or performance-based testing must be used to measure the knowledge and/or skills acquired from training programs.

Training Content

The content of training (initial, refresher, and on-the-job) must be consistent with the knowledge and skills required to perform assigned S&S tasks and/or responsibilities. Performance testing of individual and small unit tactics must be performed as part of initial, refresher, and on-the-job training (OJT) for the PF.

Training Course Development

A systematic approach must be used to produce training products that ensure the individual acquires the knowledge and skills necessary to perform their assigned duties. The approach used must have the following phases: analysis, design, development, implementation, and evaluation.

- Analyses must be conducted to ensure that training courses reflect the requirements of the job competencies. Training requirements must be determined by analyzing needs, the job or function, or performance deficiencies.
    - Needs analyses must be conducted in response to identified performance problems to validate the need for training.

- Job analyses must identify critical tasks. Job analyses will determine the frequency and method of training.
- Analysis must include determination of delivery method to ensure the most effective training outcomes.

- Design—instructional objectives must be developed based upon the skills and knowledge associated with a task and must form the basis for the development of all training materials, tests, and strategies.
- Development:
  - Lesson plans must reflect instructional objectives to ensure consistent achievement of those objectives each time the course is taught.
  - Course design documents and training materials used to support instructional objectives must be technically accurate and current.
- Implementation:
  - Training will be conducted using certified instructors who have appropriate experience and/or training to ensure the accomplishment of instructional objectives. Instructor certification will be obtained through the DOE NTC. Instructors will be recertified at least once every 2 years (at least every 24 months) to maintain technical proficiency.
  - Qualified personnel whose past experience in training is such that they may be exempted from training may be allowed to do so on a case-by-case basis through testing or equivalency. When testing is used for this purpose, it will consist of the same or equivalent examinations based on instructional objectives as stated for the required training course.
  - Completion of testing or granting of equivalency will be documented in the training records system.
- Evaluations of training must be performed to ensure that instructional objectives are met and to determine the overall effectiveness.

Training Approval Program

TAP is a process to ensure that established objectives, standards, and criteria are met by validating, through the Office of Security, security training programs conducted by organizations other than the NTC.

- Upon the request of the departmental element the NTC will certify site implementation of NTC-developed courses.
- Site programs must be examined by representatives of the NTC every 5 years (at least every 60 months) to verify adherence to departmental training objectives and standards and to provide program approval recommendations to the Director, Office of Security.
- Initial and recurring reviews for training approval must cover all aspects of local training programs including program management and structure, course content, training facilities, observation of course presentations for effectiveness, and evaluation of students.
- Training approvals will remain valid for a period of 5 years.

- TAPs must be re-evaluated and resubmitted for approval based upon significant changes in operational missions or conditions.

Training Records Management

- Training records will be maintained.
- Training records must contain dates of course attendance, course title, and scores/grades achieved, where applicable.
- Training records may be retained in electronic or hardcopy form.
  - Training provided at the NTC must be recorded by the NTC and the organization sponsoring the individual.
  - Records of training provided at other facilities, including contractor or other government facilities, must be provided to, and retained by, the organization sponsoring the individual.

Training Plans

Training plans that project training derived from a valid needs analysis for the forthcoming year must be developed annually for each program element. Annual training plans must be approved by the DOE CSA and must address

- training needs analysis;
- critical needs, or those immediate training needs which when met will be effective at improving organizational and workforce performance;
- training goals and objectives;
- major training delivery programs, projects, and other significant activities; and
- mandatory training and qualifications for compliance with DOE requirements and any additional requirements directed by DOE line management.

12. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the S&S Awareness Program.

a. Discuss the objectives and requirements of the S&S awareness program.

The following is taken from DOE M 470.4-1 chg 1.

Objective

The objective of the S&S Awareness Program is to inform individuals of their S&S responsibilities and to promote continuing awareness of good security practices.

Requirements

Briefings. The S&S awareness programs must include

- an initial briefing for all DOE Federal and contractor employees;
- comprehensive, refresher, and termination briefings for all Federal and contractor employees and personnel granted DOE access authorizations; and
- appropriate awareness briefings for any non-DOE personnel granted unescorted access to departmental security areas.

An individual granted a DOE access authorization must execute a "Classified Information Nondisclosure Agreement" (SF 312) or otherwise comply with 32 Code of Federal Regulations (CFR), chapter XX, "Information Security Oversight Office, National Archives, and Records Administration," before being granted access to classified information or matter.

S&S awareness programs must include supplementary activities to keep individuals aware of their responsibilities.

b. Discuss the elements required in the design and development of S&S Awareness Programs.

The following is taken from DOE M 470.4-1 chg 1.

The elements required in the design and development of S&S Awareness Programs are:

- Program Design—S&S awareness programs must include objectives designed to meet site-specific needs and Federal requirements, and ensure cleared and uncleared personnel are continuously aware of their S&S responsibilities.
- Program Development—procedures must be developed to ensure implementation of all S&S awareness program requirements.
- Program Assessment—S&S awareness programs must be assessed according to DOE M 470.4-1 chg 1, section G.

c. Discuss the types of briefings required by the S&S Awareness Program.

The following is taken from DOE M 470.4-1 chg 1.

S&S awareness briefings for cleared personnel must address site-specific needs, S&S interests, and potential threats to the facility/organization. Contents must be updated as necessary. Records must be maintained in a manner that provides an audit trail that verifies an individual's receipt of the briefings.

- Initial briefing. Personnel who receive a DOE security badge must receive an initial briefing before they are given unescorted access.
- Comprehensive briefing. An individual must receive a comprehensive briefing upon receipt of an access authorization and before receiving initial access to classified information or matter, or SNM.
- Refresher briefing. Cleared individuals must receive annual (at least every 12 months) refresher briefing. Agreements between DOE elements and/or contractor organizations may be established to ensure that individuals temporarily assigned to other DOE locations receive refresher briefings on schedule.
- Termination briefing. A termination briefing is required whenever an access authorization has been or will be terminated. Termination briefings must reiterate to the individual the continuing responsibility not to disclose classified information or matter to which they had access, the potential penalties for noncompliance, and the obligation to return all unclassified controlled and classified documents and materials in the individual's possession to the CSA or to DOE.

d. Discuss the administration, retention, and storage of the Classified Information Nondisclosure Agreement (SF 312).

The following is taken from DOE M 470.4-1 chg 1.

Administration:

- As a condition of access, a cleared individual must complete an SF 312 either at the time of, or after, the comprehensive briefing and before accessing classified information or matter.
- Any individual who refuses to execute an agreement must be denied access to classified information or matter and reported to the CSA.
- Any DOE employee can witness a DOE or contractor employee's agreement, but only an authorized DOE employee may also accept a contractor employee's agreement, or a contractor representative may be authorized in writing by the DOE cognizant authority to witness and to accept an agreement from a contractor employee on behalf of the U.S. government.

Retention

The original SF 312 or a legally enforceable facsimile must be retained according to General Records Schedule (GRS) 18, item 25, published by the National Archives and Records Administration (NARA), as supplemented by the DOE Administrative Records Schedule. The CSA must ensure SF 312s retained by contractors are sent to DOE upon the termination of employment of contractor employees.

Storage

The SF 312 must be stored according to GRS 18, item 25, as supplemented by the DOE Administrative Records Schedule. Personnel security files must not be used as a storage location for the agreements. The originals or legally enforceable facsimiles of the executed agreements must be retained in a file system from which they can be expeditiously retrieved if the U.S. government seeks enforcement or subsequent employers require confirmation of execution.

e. Discuss the purpose of the supplementary awareness activities.

The following is taken from DOE M 470.4-1 chg 1.

Purpose—supplementary S&S awareness activities must be provided between annual (at least every 12 months) and refresher briefings to ensure that individuals are aware of their S&S responsibilities.

13. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the policies and procedures contained in the Incidents of Security Concern Program.

a. Discuss the requirements for implementing the Incidents of Security Concern Program.

The following is taken from DOE M 470.4-1 chg 1.

The broad-based requirements for implementing DOE M 470.4-1 chg 1, section N, are listed below. There may be instances where security incidents are required to be reported through other Department reporting systems (e.g., Computer Incident Advisory Capability, Occurrence Reporting and Processing System).

- Any person who observes, finds, or has knowledge or information about a potential incident of security concern must immediately report this information to the facility security officer (FSO) or designee of the facility where the incident occurred. The FSO or designee must make notification as specified in DOE M 470.4-1 chg 1, chapter I, paragraph 3 of section N.
- Any person discovering a potential incident of security concern, including one that involves classified information or matter; SNM, including material protected, controlled, and accounted for as SNM; or other security interests at risk (e.g., interests not properly controlled), must make reasonable efforts to safeguard the security interests in an appropriate manner. The individual must also ensure evidence associated with the incident is not tampered with or destroyed.
- Any person discovering actual or suspected fraud, waste, or abuse of government resources must ensure such incidents are reported to the Office of the Inspector General according to DOE O 221.1A, *Reporting Fraud, Waste, and Abuse to the Office of Inspector General*, 4-19-08.
- Locally developed procedures must be established, documented, approved by the departmental element, and disseminated to ensure the identification, reporting, root cause analysis, and resolution of incidents of security concern. These procedures must also identify guidelines for corrective actions and documentation of time and funds expended on incidents.
- Inquiries must be conducted to establish the facts and circumstances surrounding an incident of security concern.
- Appropriate Federal (to include the Office of Security), state, and local organizations must be contacted when a violation of law is suspected or discovered.
- Appropriate corrective actions must be taken for each incident of security concern to reduce the likelihood of recurrence of the incident, including review and/or revision of applicable S&S plans and procedures.
- The party or parties responsible for an incident of security concern must be subject to appropriate administrative actions, including disciplinary measures, retraining, counseling, or other directed actions necessary to reduce the likelihood of recurrence of the incident.

- Any disciplinary or adverse actions involving DOE employees must be conducted according to DOE Order 3750.1 chg 6, *Work Force Discipline*.

b. Discuss the elements that provide the basis for identification and categorization of incidents of security concern.

The following is taken from DOE M 470.4-1 chg 1.

Incident identification—incidents of security concern are actions, inactions, or events that have occurred at a site that

- pose threats to national security interests and/or critical DOE assets;
- create potentially serious or dangerous security situations; potentially endanger the health and safety of the workforce or public (excluding safety-related items)
- degrade the effectiveness of the S&S program
- adversely impact the ability of organizations to protect DOE S&S interests

Incident categorization—incidents of security concern must be categorized according to their potential to cause serious damage or place S&S interests and activities at risk. Four categories of security incidents have been established based on the relative severity of the incident. Each of the four categories is identified by an impact measurement index (IMI) number as follows (from most severe to least severe): IMI-1, IMI-2, IMI-3, and IMI-4. Each of the four categories is further subdivided into specific subcategories based on the security topical areas of physical protection, PF, information security, personnel security, and MC&A. The categorization of specific security incidents occurs at the time the security incident is discovered. The categorization of specific security incidents can change based on information developed during the inquiry into the incident.

c. Define the actions, inactions, or events that apply to the four categories identified by impact measurement index numbers IMI-1 through IMI-4.

The following is taken from DOE M 470.4-1 chg 1.

The IMI number is used to identify, trend, and evaluate each security incident or combination of incidents. The basis for each IMI category is:

- IMI1—actions, inactions, or events that pose the most serious threats to national security interests and/or critical DOE assets, create serious security situations, or could result in deaths in the workforce or general public.
- IMI-2—actions, inactions, or events that pose threats to national security interests and/or critical DOE assets or that potentially create dangerous situations.
- IMI-3—actions, inactions, or events that pose a threat to DOE security interests or that potentially degrade the overall effectiveness of the Department's S&S protection program.
- IMI-4—actions, inactions, or events that could pose threats to DOE by adversely impacting the ability of organizations to protect DOE S&S interests.

d. Discuss the incidents of security concern reporting requirements.

The following is taken from DOE M 470.4-1 chg 1.

When an incident is suspected to have occurred, the CSA at the site/facility where the incident occurred has twenty-four hours to examine and document all pertinent facts and circumstances to determine whether an incident has occurred. During this period, the suspected incident must be categorized by an IMI number. If it is determined that an incident of security concern did not occur, no further action is required.

Incidents of security concern initial reports for IMI-1, IMI-2, and IMI-3 (as well as those for IMI-4 involving non-U.S. citizens, per DOE M 470.4-1 chg 1, section N, paragraph 3d) must be sent to the DOE HQ OC using DOE F 471.1, *Security Incident Notification Report*, according to locally developed procedures approved by line management. Initial security incident reports must be forwarded based on the following criteria:

- Within one hour following categorization for security incidents determined to be IMI-1, the CSA at the originating site/facility must transmit a DOE F 471.1 to the DOE HQ OC. If a verbal notification of the incident is made to the DOE HQ OC, a follow-up transmission of the DOE F 471.1 to the DOE HQ OC must still be made.
- Within eight hours following categorization of security incidents determined to be IMI-2/IMI-3, the CSA at the originating site/facility must transmit a DOE F 471.1 to the DOE HQ OC. If a verbal notification of the incident is made to the DOE HQ OC, a follow-up transmission of the DOE F 471.1 to the DOE HQ OC must still be made.

In addition to the IMI reporting time frames, the Office of Security must be notified within 8 hours of any security incidents that have been or will be reported in the media. The initial DOE F 471.1 and any subsequent updates must clearly identify the fact of media reporting.

Security incidents having any association with non-U.S. citizens must be clearly identified and reported on the initial DOE F 471.1 and subsequently in any related update or follow-on activity pertaining to the incident, including incidents categorized as IMI-4. For security incidents involving any credible information that a non-U.S. citizen or an agent of a foreign power is involved, the geographically closest element of the Office of Counterintelligence (OCI)/Office of Defense Nuclear Counterintelligence (ODNCI) must be notified.

When the initial incident notification report (i.e., DOE F 471.1) is transmitted, it must include a local incident tracking number. All subsequent reports pertaining to a security incident must be transmitted to the Office of Security. Changes in IMI categorizations require resubmission of a DOE F 471.1 (or form similar in content) to the Office of Security.

Only the initial DOE F 471.1 is required for incidents involving activities associated with sensitive programs. These programs include the SCI Program, SAP, Technical Surveillance Countermeasures Program (TSCP), Counterintelligence (CI) Program, or other programs identified by the Office of Security. All subsequent reporting must be handled "within channels" until such time as the inquiry report had been distributed. The date of the inquiry

report must be transmitted to the Office of Security for entry into the incident tracking and analyses capability database.

Closing inquiries:

- IMI-1 and IMI-2 incidents are considered closed upon completion of the inquiry report. The inquiry report must be completed within sixty working days of the incident categorization or a status report must be provided according to DOE M 470.4-1 chg 1, section N, paragraph 3k.
- IMI-3 incidents are considered closed upon completion of DOE F 5639.3, *Report of Security Incident/Infraction*, and transmission of the completed DOE F 5639.3 to the Office of Security. The completion of the section on assignment and acceptance of security incident must be completed as required in local procedures.
- IMI-4 incidents are considered closed upon completion of the DOE F 5639.3 according to associated local procedures.
- A sanitized (unclassified) copy of the DOE F 5639.3 must be provided to the responsible personnel security office for placement in the appropriate personnel security file.

Inquiry officials must forward final inquiry reports according to local procedures to line management for action and to the Office of Security.

By the tenth working day of each month, the Office of Security will e-mail a summary status report of the previous month's recorded incidents and inquiries to the CSA and departmental elements.

- New closures during the current month and all open incidents will be reflected in the monthly update.
- These monthly updates will be used to ensure the Office of Security and the CSA maintains accurate, coordinated, and reconciled incident/inquiry status information.

Status/Summary reports:

- IMI-1 and IMI-2—a monthly status report must be provided to the Office of Security and the departmental element for IMI-1 and IMI-2 incidents that have not been closed within sixty working days of notification of the incident.
  - Status reports must include at a minimum, the local tracking number, date of incident categorization, completed and planned actions, identification of issues precluding closure, and estimated date of closure. A copy of the original DOE F 471.1 (or form similar in content) may be included.
  - Status reports are due by the fifth working day of each month.
- IMI-3—status reports are not required for IMI-3 incidents.
- IMI-4—the CSA at each facility must maintain a compilation of IMI-4 incidents by month. These monthly summaries, which must contain the number of open and closed security incidents by IMI-4 subtopic, the total initiated for the calendar month, and a running total of open and closed incidents for the calendar year, must be provided to the Office of Security. If no reportable incidents occurred during the calendar month,

a summary stating "no reportable incidents" must be forwarded to the Office of Security by the fifth working day of each month.

Separate but related reporting:

- Occurrence reporting processing system. To eliminate reporting redundancy and centralize the reporting of security-related occurrences, all occurrences previously reported within the "Group 5—Safeguards and Security" category once contained in cancelled DOE M 231.1-2, *Occurrence Reporting and Processing of Operations* Information, dated 8/19/03 are now incorporated into this section. Because an event meets the criteria for reporting as an incident of security concern does not negate the responsibility to report it as an occurrence under DOE O 231.1A chg 1, *Environment, Safety, and Health Reporting*, 6-3-04 (i.e., event affects both safety and security).
- DOE O 151.1C, *Comprehensive Emergency Management* System, dated 10/29/2003. Incidents that are reportable under the provisions of DOE O 151.1C must continue to be reported according to that order and DOE M 470.4-1 chg 1, section N.
- NNSA "Flash Reporting" procedures are not affected by the requirements in DOE M 470.4-1 chg 1, section N.
- Under certain circumstances, related incidents of security concern, that are anticipated to recur over a long period of time, may be consolidated into a single monthly report. This situation will be handled on a case-by-case basis between the CSA, the departmental element, and the Office of Security. Specific plans for this reporting process must be developed by the CSA and submitted through the departmental element to the Office of Security.

Corrective actions identified in response to an incident of security concern must be documented. For incidents categorized as IMI-1, IMI-2, or IMI-3, a copy of the documentation must be forwarded to the Office of Security if this information is not included in the inquiry report. Documentation on corrective actions for IMI-4 incidents does not have to be forwarded to the Office of Security.

The Defense Authorization Act, 43 CFR 3150, "Offshore Oil and Gas Geophysical Exploration," requires the Secretary of Energy to notify the Committees on Armed Services of the Senate and House of Representatives of each "significant nuclear defense intelligence loss." A "significant nuclear defense intelligence loss" is defined in the Defense Authorization Act as "any national security or CI failure or compromise of classified information at a facility of the Department or operated by a contractor of the Department that the secretary considers likely to cause significant harm or damage to the national security interest of the U.S."

- The Department regards the loss or compromise (i.e., disclosure of classified information to unauthorized persons) of TS information; SCI; SAP information; and weapon data Sigmas 1, 2, 14, and 15 as reportable under Section 3150.
- Within thirty days of discovery of Section 3150 reportable incidents, the Office of Security, after consultation with the Director, Central Intelligence, and the Director, FBI, must provide notification to Congress.

e. Discuss the authorization and limits of authority of inquiry officials.

The following is taken from DOE M 470.4-1 chg 1.

Inquiry officials must conduct inquiries to establish the pertinent facts and circumstances surrounding incidents of security concern.

Inquiry officials may be either Federal or contractor employees but must have previous investigative experience or Department inquiry training and must be knowledgeable of appropriate laws, executive orders, departmental directives, and/or regulatory requirements.

- Contractors may conduct inquiries into incidents of security concern; however, if a violation of law is determined or suspected or the inquiry establishes information that a foreign power or an agent of a foreign power is involved, the contractor must stop further inquiry actions and notify the DOE CSA, which will assume further notification and reporting responsibilities, to include coordination with OCI/ODNCI. In such instances, the contractor must document the known circumstances surrounding the incident of security concern and submit all accumulated data to the DOE CSA.
- In all instances where the DOE CSA disagrees with the contractor report, the DOE CSA must assume supplemental inquiry responsibilities.
- When the inquiry into an incident of security concern necessitates communication with agencies/organizations external to the Department, a Federal employee must be responsible for performing all such communication.
- Contact with Federal, state, and local law enforcement officials may be made by contractors with the written concurrence of the DOE CSA and DOE line management.

Inquiry officials are not authorized to detain individuals for interviews or obtain sworn statements; however, they may conduct consensual interviews and obtain signed statements.

Inquiry officials must be appointed in writing by the DOE line management, the head of the Office of Headquarters Security Operations, or the Office of Security.

Inquiry officials are responsible for conducting the inquiry and maintaining records and documentation associated with the inquiry (e.g., logs of events, notes, recordings, and statements).

When inquiry officials discover suspected or confirmed violations of law, they must immediately notify the Office of Security.

f. Discuss the policies and procedures for cooperating with Federal, state, and local law enforcement personnel.

The following is taken from DOE M 470.4-1 chg 1.

If a violation of law has occurred and the preservation of evidence requires the immediate notification of Federal, state, or local law enforcement agencies, the DOE CSA must perform all necessary referrals and notifications, including notification to the Office of Security. The Office of Security will notify the HQ elements of all referrals to other Federal law enforcement agencies, including the FBI.

Federal, state, or local law enforcement agency personnel requiring access to limited areas (LAs) or higher for investigative actions must be escorted, have a current access authorization pass to DOE, or possess an active DOE access authorization. Such personnel will be approved for access to classified information or matter only if they possess the appropriate access authorization, the matter directly pertains to the investigation, and appropriate programmatic approvals have been granted, if such approvals are required. Access to RD and Formerly Restricted Data (FRD) requires a DOE Q or L or appropriate personnel security clearance.

When authorized and approved Federal, state, or local law enforcement personnel are given access to classified information, they must be immediately advised of the classification level and category. They must also be informed of the protection and control requirements associated with the classified information they possess.

When an inquiry establishes information that a foreign power or an agent of a foreign power is involved, the Office of Security must immediately notify OCI/ODNCI, which in turn will notify the FBI according to 50 U.S.C. 402a, "Counterintelligence and Security Enhancements Act of 1994."

When an inquiry surrounding an incident of security concern establishes information indicating that fraud, waste, or abuse has occurred, the Office of the Inspector General must be notified for information and/or action.

The DOE CSA must make arrangements for the issuance of standard DOE security badges, the granting of access to classified information, and any other necessary agreements or items requested or required by Federal, state, or local law enforcement agencies involved in investigations.

g. Discuss the criteria used to determine the lead organization responsible for conducting an inquiry of an incident of security concern.

The following is taken from DOE M 470.4-1 chg 1.

If an incident affects more than one site/facility, the following criteria must be used in determining the lead organization responsible for conducting the inquiry:

- If the sites/facilities fall under the purview of a single DOE CSA, that DOE CSA must assign responsibility to a lead organization.

- If the sites/facilities fall under the purview of multiple DOE CSAs, those DOE CSAs must, by mutual agreement, decide on a lead organization with responsibility for the inquiry.

h. Describe the actions that must be taken when conducting inquiries into incidents of security concern.

The following is taken from DOE M 470.4-1 chg 1.

The following actions must be taken when conducting inquiries into incidents of security concern and be reflected in the inquiry report.

Data collection:

- Collect all data/information relevant to the incident, such as operations logs, inventory reports, requisitions, receipts, photographs, signed statements, etc.
- Conduct interviews to obtain additional information regarding the incident.
- Collect physical evidence associated with the inquiry, if available. (Examples of physical evidence include, but are not limited to, recorder charts, computer hard drives, defective/failed equipment, procedures, and readouts from monitoring equipment, etc.)
- Ensure physical evidence is protected and controlled and a chain-of-custody is maintained).

Incident reconstruction:

- Reconstruct the incident of security concern to the greatest extent possible using collected information and other evidence.
- Develop a chronological sequence of events that describes the actions preceding and following the incident.
- Identify persons associated with the incident.

Incident analysis and evaluation—this analysis determines which systems/functions performed correctly or failed to perform as designed. It provides the basis for determining the cause of the incident and subsequent corrective actions. Inquiry officials must

- analyze the information collected during the inquiry to determine whether it describes the incident completely and accurately
- collect additional data and reconstruct the incident if more information is required
- identify any collateral impact with other programs or security interests

i. Discuss the inquiry report content/closure consideration and administrative actions.

The following is taken from DOE M 470.4-1 chg 1.

Inquiry reports must describe the conduct and results of the inquiry and include the following information for the incident to be closed:

- An executive summary.

- A narrative, which must include the following items:
  - Date and time of incident discovery, any notifications, the incident inquiry, and other time-related actions pertaining to the incident (WHEN).
  - All data pertinent to the location of an incident, including the facility name and code (as registered in the SSIMS), building/room numbers, and other identifying information as appropriate. Such information is required for all facilities affected by the incident (WHERE).
  - A complete discussion of the facts and circumstances surrounding the incident, including a description of all supporting information (WHAT), such as the following:

    - Detailed description of the incident of security concern.
    - Identification of all personnel involved in the incident and when they were notified, including those associated with the inquiry process (i.e., inquiry officials and assisting personnel).
    - Identification of the causes for the incident (direct and contributing factors) and descriptions of the mitigating or aggravating factors that may reduce or increase the impact of the incident.
    - Description of the actions that precipitated the incident.
    - Description of all physical evidence, including all records/documents reviewed (e.g., training records, policies/procedures).
    - Results of any interviews performed.
    - Descriptions of actions taken to minimize vulnerabilities created by the incident and prevent further loss/compromise of the security interest.
    - If the incident involves classified information or matter, the following must also be included.

      A description of the potentially compromised classified information or matter, including but not limited to, classification level, category, caveats (if any), and form of information (e.g., document title, date, and description). [A copy of the evidence (or photograph) must be retained and provided to the Office of Security, if requested.].
      The classification guide and topic or source document, including date, of guide or source document.
      Known recipients of potentially compromised matter.
      Owner of the classified information or matter (e.g., program office or OGA).

  - An inquiry official's conclusion and the basis/facts that support the conclusion are essential.

    - Given the facts determined through the inquiry, the conclusion of the final report must address the potential risk to the security interest based upon a subjective analysis of the facts and circumstances surrounding the incident of security concern.

- The final report must also identify the line management responsible for corrective actions and disciplinary actions.

- The following must be included as attachments to the report of inquiry:
  - A copy of the documentation appointing the inquiry official
  - A copy of any signed statements of involved individuals
  - A description of the compromised or potentially compromised information (as appropriate)
  - A copy of the DOE F 471.1 and other documents obtained during the data collection phase of the inquiry
  - A copy of any DOE F 5639.3, or a form comparable in content, issued as a result of the inquiry
  - A copy of any DOE F 5639.2, *Reporting Unaccounted for Documents*, or a form comparable in content, if applicable

Administrative Actions

- Whenever possible, the responsibility for an incident of security concern must be assigned to an individual rather than to a position or office.
  - When individual responsibility cannot be established and the facts show that a responsible official allowed conditions to exist that led to an incident of security concern, responsibility must be assigned to that official.
  - Security infractions are issued to document the assignment of responsibility for an incident of security concern. Individuals who do not possess an access authorization may be issued a security infraction.
- Corrective actions taken in response to incidents of security concern must be documented, and for incidents categorized as IMI-1, IMI-2, and IMI-3, a copy of the documentation must be forwarded to the Office of Security. Documentation on corrective actions for IMI-4 incidents does not have to be forwarded to the Office of Security.
- A copy of part 1 of DOE F 5639.3, or a similar form, must be placed in the employee's DOE personnel security file. If an employee does not have an access authorization, it must be placed in his/her personnel file.

j. Discuss the requirements for the retention of records pertaining to incidents of security concern.

The following is taken from DOE M 470.4-1 chg 1.

Records pertaining to incidents of security concern must not be sent to Federal Records Centers. Records must be dispositioned according to an applicable GRS, published by the NARA, or according to a DOE records disposition schedule approved by NARA, whichever is applicable. The site records manager or similarly titled person should be routinely consulted regarding the maintenance and disposition of records.

k. Discuss the requirements for inquiries into compromise of, potential compromise of, or missing classified information.

The following is taken from DOE M 470.4-1 chg 1.

The following requirements are in addition to those contained in DOE M 470.4-1 chg 1, section N, chapter 1. Inquiry officials must perform the following actions:

- Interview custodians and others having knowledge of the incident. When necessary, records must be audited for evidence of destruction, transmission, or other disposition.
- Ensure a DOE F 5639.2, or a form comparable in content, is completed if classified information or matter is missing.
- Determine which departmental element has programmatic responsibility for the information or whether the information was originated by another government agency or foreign government.
- Determine whether a compromise or potential compromise occurred. If there was a potential compromise, seek to determine the probability of compromise. Document the basis for such findings (i.e., potential compromise is defined as an incident of security concern where circumstances exist that cannot rule out the compromise of classified information).
- If an inquiry determines that a compromise or potential compromise has occurred, document the extent of the dissemination of the classified information and the actions taken to prevent further dissemination.
- When an inquiry establishes that classified information has been compromised by being published in the media, the questions contained in the Department of Justice (DOJ) eleven-point criteria, which are listed below, must be answered and coordinated with the Office of Security. When completing the questions, provide all documentation and appropriate information to support affirmative responses. Each question must be answered affirmatively before the DOJ will initiate a formal investigation into the compromise; however, failure to affirmatively answer all the DOJ criteria does not preclude the DOJ from pursuing administrative or criminal action.
    - Could the date and identity of the article or articles disclosing the classified information be provided?
    - Could specific statements in the article that are considered classified be identified? Was the data properly classified?
    - Is the classified data that was disclosed accurate? If so, provide the name of the person competent to testify concerning the accuracy.
    - Did the data come from a specific document, and, if so, what is the origin of the document and the name of the individual(s) responsible for the security of the classified data disclosed?
    - Could the extent and official dissemination of the data be determined?
    - Has it been determined that the data has not been officially released in the past?
    - Has it been determined that prior clearance for publication or release of the information was not granted by proper authorities?

- Does review reveal that educated speculation on the matter cannot be made from material, background data, or portions thereof which have been published officially or have previously appeared in the press?
- Could the data be made available for the purpose of prosecution? If so, include the name of the person competent to testify concerning the classification.
- Had it been determined that declassification had not been accomplished prior to the publication or release of the data?
- Will disclosure of the classified data have an adverse impact on the national defense?

l. Discuss the purpose for damage assessments when classified information has been compromised.

The following is taken from DOE M 470.4-1 chg 1.

Damage assessments determine potential damage to national security when classified information has been compromised or potentially compromised. Damage assessments are performed to evaluate and document possible countermeasures and conduct actions to limit potential damage. The departmental element must use the damage assessment to determine future courses of action within the affected program. Additionally, damage assessments are used by appropriate authorities when criminal prosecution is sought. Classification guidance must be evaluated and updated, as appropriate, based on damage assessments. Damage assessments must be conducted when

- inquiries disclose evidence that classified information, including weapon data, SCI, or SAP data have been compromised or potentially compromised;
- analyses reveals similar information has been compromised frequently or when the information has been compromised to a wide audience (e.g., public media, international conference, Internet);
- a violation of laws appears to have occurred and criminal prosecution is contemplated; or
- the departmental element determines one is necessary.

m. Discuss the required damage assessment procedures and the contents of the damage assessment reports.

The following is taken from DOE M 470.4-1 chg 1.

The following damage assessment procedures must be followed:

- The originator of the compromised information must provide the DOE CSA with a copy of the compromised or potentially compromised information, if available. If no other copy exists, the originator must provide a detailed description of the compromised information.
- The originator must coordinate with a derivative classifier to confirm the classification level and category of the compromised information according to current

classification guidance and policy. The derivative classifier must provide the basis for the classification determination (i.e., the classification guide used).

- The team performing the damage assessment must prepare a draft assessment and coordinate it with the originator of the compromised or potentially compromised information.
- The damage assessment must be approved by the departmental element with programmatic responsibility for the compromised or potentially compromised information, and at a minimum, copies will be submitted to the Director, Office of Security and the DOE CSA responsible for the inquiry. The Director, Office of Security will coordinate with the departmental element and distribute additional copies, as appropriate.

Damage assessment reports must contain the following information:

- Identification of the source, date, and circumstances of the compromise or potential compromise.
- Classification of the specific information compromised or potentially compromised.
- Description of the specific information compromised or potentially compromised.
- Analysis and statement of the known or probable damage to national security that has resulted or may result.
- Analysis and statement of the known or probable impact to the affected program.
- Assessment of the possible advantage to foreign governments and/or hostile organizations as a result of the compromise or potential compromise.
- Recommendation to the Office of Classification and Information Management Control regarding whether the classification of specific information should be modified to minimize or nullify the effects of the reported compromise or potential compromise, to include downgrading, declassification, or upgrading.
- Assessment of whether countermeasures are appropriate and feasible to negate or minimize the effect of the compromise or potential compromise.
- Assessment of other appropriate corrective actions.

Damage assessments may be completed for a group of similar incidents when such grouping is a logical method of meeting this requirement. A logical grouping includes a situation where multiple matters requiring a damage assessment are related to a programmatic area and would result in the same or similar damage to national security or advantage to foreign governments and/or hostile organizations.

Whenever a compromise or potential compromise involves the classified information of an OGA, the DOE CSA responsible for the inquiry must provide the facts and circumstances that affect the OGA's information or interests to the Director, Office of Security. The Director, Office of Security, must coordinate with the OGA, as appropriate.

Whenever a compromise or potential compromise involves the information of a foreign government that requires protection (e.g., Confidential Foreign Government Information Modified Handling [C/FGI-Mod]), the DOE CSA responsible for the inquiry must provide the facts and circumstances that affect the foreign government's information or interests to

the Director, Office of Security. The foreign government, however, will not normally be advised of any departmental security system vulnerabilities that allowed or contributed to the compromise or potential compromise. The Director, Office of Security will coordinate with the Department of State and the foreign government, as appropriate.

Whenever a compromise or potential compromise involves classified information or interests of more than one government agency, the following requirements apply:

- Each government agency is responsible for conducting the assessment of damage resulting from its compromised or potentially compromised information.
- If a compromise or potential compromise involves the classified information of DOE and another government agency, and if more than one damage assessment is performed, the departmental element responsible for the department's damage assessment must provide the damage assessment to the Director, Office of Security, who will coordinate with the OGA.
- When a joint damage assessment is to be made, the Office of Security will coordinate assignment or responsibility between the Department and the OGA.
- If a compromise or potential compromise of departmental classified information is the result of actions taken by non-U.S. citizens, foreign government officials, and/or U.S. nationals employed by international organizations, the Director, Office of Security, through coordination with OCI/ODNCI, must ensure, through appropriate intergovernmental liaison channels, that information pertinent to the assessment is obtained.
- If a compromise or potential compromise of SCI has occurred, the Director, Office of Intelligence must consult with the designated representative of the Director, Central Intelligence and other officials responsible for the information involved.

14. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the policies and procedures contained in the Control of Classified Visits Program.

a. Discuss the procedures that must be in place at the local level for the control of classified visits.

The following is taken from DOE M 470.4-1 chg 1.

Line management must establish local procedures for the control of classified visits. Procedures must ensure the following actions:

- Verification of the visitor's identity, programmatic need-to-know, and that the visitor's clearance or access authorization is at least equal to the classification of the information to which access is being requested.
- Identification of limitations and enforcement of controls for access to classified information or matter or facilities and submission of appropriate forms, requests, etc., to the CSA and programmatic line management within the timeframes below.

- Visit requests must be submitted at least fifteen working days before the date of a one-time visit or the first day of a recurring visit.

  - DOE and DOE contractor employees—DOE F 5631.20, *Request for Visit or Access Approval*, must be used by DOE Federal and contractor employees to obtain programmatic approval for Sigma access. This form does not need to be submitted to visit Department facilities. A DOE security badge will serve as evidence of DOE access authorization.
  - OGA and OGA contractor employees—DOE F 5631.20 (or a form similar in content) must be used by employees of OGAs to obtain access approval for visits to DOE facilities.

- Exceptions to required processing times will be allowed only for emergency visits (i.e., visits that must take place as a matter of urgency and importance and the processing lead time cannot be met). Emergency visits will only be approved as one-time visits.
- Requests for visits/access to weapons programs, nuclear materials production facilities, or sensitive nuclear materials production information must be referred to the Associate Administrator for Defense Nuclear Security.
- Requests for visits/access to uranium enrichment plants or facilities engaged in uranium enrichment technology development, including advanced isotope separation technology, must be referred to the Office of Nuclear Energy, Science, and Technology.
- Requests for access to naval nuclear propulsion facilities must be referred to the Deputy Administrator for Naval Reactors.

- Continuing visitor access approval is necessary for individuals who frequently visit DOE facilities. However, the access approval cannot exceed a period of one year or the final day of a contract for contractors, whichever is less. The approval may be renewed annually.
- Operational approval of visits.
- Maintenance of documentation associated with all classified visits/access.
  - Records of classified visits by employees and contractors of OGAs must be maintained.
  - Records of classified visits by DOE Federal and contractor employees that entailed Sigma access must be maintained.
  - Records of requests for classified visits by DOE Federal and contractor employees to OGAs must be maintained.
- Referral of any nonroutine, written, or visual material resulting from classified visits and proposed for public release to the Director, Public Affairs.
- Limiting the sending and receiving of a classified visit request to the security office of OGAs.

b. Discuss the policies and procedures for classified visits by Departmental employees, contractors, and subcontractors.

The following is taken from DOE M 470.4-1 chg 1.

Classified visits by departmental employees, contractors, and subcontractors.

- Visitors are responsible for making administrative arrangements and obtaining approval from the departmental element, as appropriate. (The authority granting such approval is responsible for informing the facility to be visited.)
- Contractors or subcontractors with mutual program interests may be authorized, subject to the limitations in DOE M 470.4-1 chg 1, section L, paragraph 2b(3), to arrange for visits without obtaining Department approval if such authorization will be advantageous to the Department.
- Visitors who require access to weapon data (classified Secret (S) or Top Secret (TS)), TS information (non-weapon data), sensitive nuclear materials production information, inertial confinement fusion data, atomic vapor laser isotope separation technology, uranium enrichment technology, or facilities specifically designated by a departmental element, must obtain approval.
    - Family visits—when the classified visit is under the auspices of a departmental element, the programmatic approval for the visit must be obtained from the departmental element exercising jurisdiction over the facility.
    - HQ visits—when the classified visit is under the auspices of line management, the programmatic approval for the visit must be obtained from both the responsible line management and the departmental element being visited.

c. Discuss the policies and procedures for classified visits to Department of Defense (DoD) and National Aeronautics and Space Administration (NASA) facilities.

The following is taken from DOE M 470.4-1 chg 1.

DoD and NASA accept DOE access authorizations for RD and other classified information or matter under their jurisdictions on the same basis as the Department, if access authorization and need-to-know are properly certified.

- DOE TS approvals must be specifically certified in the event access to TS information is required.
- A DOE F 5631.20 must be forwarded directly to the military or civilian official with jurisdiction over the information to which access is being requested.
- Any exchange of RD occurring during the course of a visit must be accomplished as stated in DOE M 470.4-1 chg 1, section L, paragraph 2e.

d. Discuss the policies and procedures for Restricted Data (RD) visits by Nuclear Regulatory Commission (NRC) employees.

The following is taken from DOE M 470.4-1 chg 1.

Visits to DOE facilities by NRC employees, consultants, contractors, or subcontractors who require access to weapon data, sensitive nuclear materials production information, atomic vapor laser isotope separation technology, or uranium enrichment technology or entry into a Department classified weapon or production facility must

- be arranged through the departmental element coordinating the visit
- have prior approval of the Associate Administrator for Defense Nuclear Security if visiting classified weapon or production facilities
- have necessary clearance verification and certification by the NRC Director of Security that access to the information requested is required in performance of official duties

Visits involving access to RD not requiring prior approval from the departmental element exercising jurisdiction over the facility or the office to be visited may be arranged directly by the NRC with the departmental element provided this procedure does not conflict with the existing visitor control procedures of the CSA.

The NRC identification badge must not be used as authority for visits in lieu of the aforementioned specific visit approval arrangements.

e. Discuss the policies and procedures for RD and other classified visits by DoD, NASA, and OGA employees.

The following is taken from DOE M 470.4-1 chg 1.

Access to RD is contingent upon submission of a DOE F 5631.20; NASA Form 405, *Request for Access Approval*; or a memorandum or electronic message signed by or in the name of the certifying official. The request must be forwarded for approval or other action to the departmental element with jurisdiction over the information to which access is requested.

Requests for access must include

- names, citizenship, dates of birth, and social security numbers of persons requesting access and organizations represented (if not Armed Services, relationship to DoD or NASA);
- facility and information to which access is requested (access to critical nuclear weapon design information must be specified as requested);
- security clearance or access authorization status of each person, including clearance data;
- purpose of visit and certification that the person needs the access in the performance of duty;
- anticipated date of visit and names of persons to be visited (if a conference is involved, the date, place, and sponsor of the conference must be specified); and
- a certification that the matter to which access is requested relates to aeronautical and space activities, for requests from NASA.

The approving official must have the authority to approve such access.

Control of access to RD in the custody of another Federal agency by members of the Armed Services or by DoD or NASA personnel or contractors is the responsibility of the appropriate official or his/her designee.

Other classified visits by DoD and NASA employees:

- Requests for such visits to DOE, contractor, and subcontractor facilities are approved by line management, or in the case of HQ elements, by the cognizant departmental element after ensuring that each visitor has the appropriate military or NASA security clearance and requires the information in the performance of their duties.
- Certification of security clearances may be made by memorandum, electronic message, DOE F 5631.20 or NASA Form 405.

Classified visits by employees of OGAs:

- Requests for visits to DOE facilities by employees, contractors, or subcontractors of Federal agencies other than DoD, NASA, or NRC are approved by the CSA.
- RD may not be exchanged with persons in this category unless they have appropriate DOE access authorization.
- Classified information or matter, other than RD, may be exchanged provided the individual has the appropriate Q or L access authorization or a security clearance granted under the provisions of Executive Order 12968, *Access to Classified Information*, and need for such access has been verified.
- Certification of security clearances for RD access must be made on DOE F 5631.20.

f. Discuss the policies and procedures for Congressional and State classified visits.

The following is taken from DOE M 470.4-1 chg 1.

Requests for visits to DOE, contractor, or subcontractor facilities by members or employees of Congress or congressional committees and by governors or their staffs must be approved by the departmental element with jurisdiction over the facilities to be visited, provided the following are verified:

- Visitor's identity
- Access authorization or security clearance
- Need-to-know.

g. Discuss the policies and procedures for emergency visits to classified areas and facilities.

The following is taken from DOE M 470.4-1 chg 1.

Emergency visits to classified areas and facilities:

- In an emergency, requests for visit approval may be made by telephone or electronic message.
- Telephone requests must be confirmed by memorandum or electronic message.

15. Safeguards and security personnel with the responsibility for PP&M must demonstrate a working level knowledge of the Unclassified Visits and Assignments of Foreign Nationals Program.

a. Describe the policies and procedures for requesting, processing, and approving visits and assignments by foreign nationals.

The following is taken from DOE O 142.3 chg 1.

Foreign national access to DOE sites, programs, information, and technologies will be approved provided the access is needed to support the program objectives of DOE and/or U.S. national interests. Sufficient documentation of immigrant or nonimmigrant status, identity and citizenship is required for all foreign visitors and assignees at all DOE sites, facilities, and laboratories to verify the foreign national's identity and authority to work and ensure that the foreign national is eligible to be in the U.S.

The passport, visa, and/or other U.S. Citizenship and Immigration Services (USCIS) information that has been provided to verify identity, authority to work, and lawful immigration status must be documented in the foreign access central tracking system (FACTS) and reviewed annually for all foreign national assignees, including nonsensitive country nationals, sensitive country nationals (individuals who were born in; are citizens of; or represent a company, business, organization or institute from countries identified as sensitive), and nationals of state sponsors of terrorism (individuals who were born in; are citizens of; or represent a company, business, organization, or institute from countries identified as state sponsors of terrorism).

Each foreign national visit or assignment must be covered by an approved security plan that addresses the sensitivity factors (including area type to be visited, determination of whether information containing sensitive subjects will be shared, and affiliation with sensitive countries or countries identified as state sponsors or terrorism) and the results of SME reviews consistent with the specific requirements of DOE O 142.3 chg 1.

SMEs will review requests for foreign national visits and assignments when required. These reviews include

- security, including CS, technical security, and operations security (OPSEC), and determination of sufficiency of the security plan for the specific visit or assignment;
- export control and determination of export license requirements;
- technology transfer;
- counterintelligence; and
- intelligence, when there is a field intelligence element onsite.

SME reviewers will consider factors associated with the requested access to DOE sites, programs, information, and technologies, including building access and surrounding activities and determinations of whether legal and policy-related terms and conditions associated with the proposed visit or assignment have been met. SME reviewers will ensure

that any identified risk to the government associated with access approval for each visit or assignment has been appropriately evaluated and mitigated.

All unclassified foreign visits and assignments (UFVAs) involving nationals or state sponsors of terrorism, sensitive country nationals, sensitive subjects, or security areas other than laboratories or facilities that perform no classified work and at which no classified materials are stored or PPAs require indices checks, which are coordinated by the Office of Intelligence and Counterintelligence.

Indices checks are requested electronically through the process of documenting visit and assignment access requests in FACTS. In cases where indices checks must be completed before access approval determination, the request must be documented 30 days before the first day of access. In cases when there is insufficient time to complete an indices check before the first day of access, the approval authority may request a CI consultation in lieu of the completion of indices check for sensitive country and nonsensitive country nationals. Counterintelligence consultations may not be employed as a standard alternative to indices checks; nor may they be used in lieu of indices checks for national of state sponsors of terrorism.

All foreign national access to DOE, programs, information, and technologies for unclassified purposes must be approved by either the Secretary of Energy or an assigned approval authority. Access approvals are subject to validation and verification of the information submitted for the access request when the visit or assignment begins.

For all foreign national access approval requests, the following apply:

- The approval authority must take into consideration all information from the review process, including SME reviews, and must evaluate potential impacts on local site operations.
- Determination of access approval must ensure that any identified risk to the government associated with the access granted has been appropriately evaluated and mitigated.
- For the request to be approved, it must be determined that the benefits to the government are greater than the risks associated with the presence of the foreign national at a DOE site. If the request is for a national or state sponsor of terrorism, it must be determined that the potential visit or assignment is extraordinary.
- Legal and policy-related terms and conditions associated with the proposed visit or assignment must be met before approval. Those terms and conditions include, but are not limited to, consideration for other activities at the site, visa sponsorship requirements, visa status conditions and requirements, right-to-work requirements, and international agreements.
- Approval determinations will be documented in FACTS. Documentation will include the date of the determination, whether the request was approved or denied, and the name of the approval authority.

Approvals for foreign national access must be consistent with line management accountability requirements.

- Approval authorities must be U.S. citizens.
- Line management accountability flows from the Secretary through the Deputy Secretary or under secretaries, to program secretarial officers (PSOs), to the head of the DOE field element, to the site management official or laboratory director for the hosting site, who has been assigned specific authority and responsibility to approve access. When the site management official or laboratory director is not a U.S. citizen, the head of the cognizant DOE field element will assign the approval authority. Final approval authority can be assigned to hosting site management officials or laboratory directors for access requests for sensitive country nationals and nonsensitive country nationals. For a hosting site management official or laboratory director to further assign approval authority, he or she must first develop a plan and related procedures for that assignment. The plan must be approved by the head of the cognizant DOE field element. Once the plan is approved, approval authority may be re-assigned to another U.S. citizen employee. All assignments of approval authority must be in writing and be promulgated by the approval authority, and copies must be provided to the cognizant DOE field element and lead program secretarial officer, the hosting site foreign visits and assignments office, and the Office of Health, Safety and Security. Site management officials and laboratory directors will be held accountable for all approval decisions made by themselves or by those to whom they re-assign approval authority. Employees to whom approval authority has been re-assigned may not further re-assign this authority.
- HQ staff and support office accountability flows from the Office of the Secretary to heads of program offices. Final approval authority can be assigned to HQ heads of program offices for access requests for sensitive country nationals and nonsensitive country nationals. The head of a HQ staff or support office may re-assign his or her approval as appropriate. All re-assignments of approval authority must be in writing, and a copy must be provided to the Office of Health, Safety and Security. Heads of HQ staff and support offices will be held accountable for all decisions made by themselves or by those to whom they re-assign approval authority. Employees to whom approval authority has been re-assigned may not further re-assign this authority.
- Access requests for nationals of state sponsors of terrorism require approval by both the site approval authority and the sponsoring HQ program office before final approval determination. Final approval authority is held by the Secretary of Energy and can only be assigned to the Under Secretary for Nuclear Security/Administrator for the National Nuclear Security Administration, Under Secretary of Energy or Under Secretary of Energy or Under Secretary for Science.
- The Office of Foreign Visits and Assignments will coordinate reviews by the HQ Offices of Health, Safety and Security; Intelligence and Counterintelligence; Defense Nuclear Nonproliferation; and any other reviews required by DOE security directives before submitting requests for review and final approval determination.

b. Describe the controls in place regarding the issuance of access badges for foreign nationals.

The following is taken from DOE O 142.1.

Foreign nationals are not badged at a DOE clearance level higher than the foreign national's authorized access. If there is no equivalent DOE clearance level, the foreign national is badged as uncleared.

c. Discuss the appropriate policies and procedures for escorting foreign nationals.

The following is taken from DOE O 142.3 chg 1.

An escort is a DOE employee who is assigned responsibility for a foreign national working or traveling within a site/facility to ensure there is no unauthorized access. With the exception of authorized hosts at laboratories or facilities that perform no classified work, and at which no classified materials are stored, sensitive country foreign nationals may not serve as escorts. Escorts are responsible for the following:

- Familiarity with the site/facility, including security areas
- Full understanding and knowledge of security plan requirements
- Knowledge of specific information or technologies to which the foreign national has been authorized access to ensure that there is no unauthorized access
- Appropriate clearance required for escort duties as required by hosting the security

d. Describe the system for communicating between the various site organizations to ensure appropriate control and oversight of foreign nationals.

The following is taken from DOE O 142.3 chg 1.

FACTS is the Department's official national database of information on UFVAs. Access to FACTS is limited to U.S. citizens. All UFVAs that require documentation will be documented in FACTS. The designated approval authority is responsible for ensuring that documentation occurs.

e. Describe the proper use of specific security plans for foreign nationals or generic plans and whether those plans need to be reviewed and by whom.

The following is taken from DOE O 142.3 chg 1.

Each foreign national visit or assignment must be covered by an approved security plan that addresses the sensitivity factors (including area type to be visited, determination of whether information containing sensitive subjects will be shared, and affiliation with sensitive countries or countries identified as state sponsors of terrorism) and the results of SME reviews consistent with the specific requirements of DOE O 142.3 chg 1.

- A security plan is required to address specific site security concerns relating to foreign national visits or assignments. Specific security plans are required for access

by foreign nationals to areas other than laboratories or facilities that perform no classified work and at which no classified materials are stored or PPAs, for access to information on the sensitive subject list, or for foreign national affiliation with a sensitive country (with the exception of laboratories or facilities that perform no classified work, and at which no classified materials are stored) or a country identified as a state sponsor of terrorism. A specific security plan is also required if the SSSP or SSP does not provide sufficient protection of DOE facilities, programs, and information for the conduct of the foreign national visit or assignment. The specific security plan must be approved by the site security representative and by the site approval authority and will be used in conjunction with the SSSP or SSP.

- Generic security plan—if an SME review determines that none of the requirements for a specific security plan exist, and that the SSSP or the SSP provides sufficient protection of DOE facilities, programs, and information for the conduct of the foreign national visit or assignment, no further documentation of security measures for that visit or assignment is required.

f. Describe the system used to contain data on foreign nationals and the information needed for inclusion.

The following is taken from DOE O 142.3 chg 1.

FACTS is the Department's official national database of information on UFVAs. Access to FACTS is limited to U.S. citizens. All UFVAs that require documentation will be documented in FACTS. The designated approval authority is responsible for ensuring that documentation occurs.

The passport, visa, and/or other USCIS information that has been provided to verify identity, authority to work, and lawful immigration status must be documented in FACTS and reviewed annually for all foreign national assignees including nonsensitive country nationals, sensitive country nationals (individuals who were born in; are citizens of; or represent a company, business, organization or institute from countries identified as sensitive), and nationals of state sponsors of terrorism (individuals who were born in; are citizens of; or represent a company, business, organization, or institute from countries identified as state sponsors of terrorism).

g. What are the prescribed timing requirements for advance notification of a visit of a foreign national?

The following is taken from DOE O 142.3 chg 1.

All UFVAs involving nationals of state sponsors of terrorism, sensitive country nationals, sensitive subjects, or security areas other than laboratories of facilities that perform no classified work and at which no classified materials are stored for PPAs require indices checks, which are coordinated by the Office of Intelligence and Counterintelligence.

Indices checks are requested electronically through the process of documenting visit and assignment access requests in FACTS. In cases where indices checks must be completed before access approval determination, the request must be documented 30 days before the first day of access.

In cases when there is insufficient time to complete an indices check before the first day of access, the approval authority may request a CI consultation in lieu of the completion of the indices check for sensitive country and nonsensitive country nationals.

h. Describe the processes in place for making changes to approved security plans for foreign nationals; for making changes in assigned escorts and how it is reported; and for submitting host reports.

The following is taken from 10 CFR 95.19.

Each licensee, certificate holder, or other person shall obtain prior CSA approval for any proposed change to the name, location, security procedures and controls, or floor plan of an approved facility. A written description of the proposed change must be furnished to the CSA and the NRC Regional Administrator of the cognizant regional office and, if the NRC is not the CSA, also to the Director, Division of Nuclear Security, Office of Nuclear Security and Incident Response; the communications to NRC personnel should be by an appropriate method. Substantive changes to the security plan must be submitted to the NRC, Division of Nuclear Security, or CSA, at least 30 days prior to the change so that they may be evaluated.

The CSA shall promptly respond in writing to all such proposals. Some examples of substantive changes requiring prior CSA approval include

- a change in the approved facility's classified mail address; or
- a temporary or permanent change in the location of the approved facility.

Approved changes will be reflected in a revised security plan submission within 30 days of approval. Page changes rather than a complete rewrite of the plan may be submitted.

A licensee, certificate holder, or other person may effect a minor, non-substantive change to an approved security plan for the safeguarding of classified information without receiving prior CSA approval. These minor changes that do not affect the security of the facility may be submitted to the addressees noted above 30 days prior to the change. Page changes rather than a complete rewrite of the plan may be submitted. Some examples of minor, non-substantive changes to the security plan include

- the designation/appointment of a new FSO; or
- a revision to a protective personnel patrol routine, provided the new routine continues to meet the minimum requirements of this part.

A licensee, certificate holder, or other person must update its NRC FCL every five years either by submitting a complete security plan or a certification that the existing plan is fully current to the Division of Nuclear Security.

The following information is taken from the Office of Counterintelligence, *Hosting Foreign Nationals at DOE Sites* booklet.

If changes in the dates of access by the foreign national, changes in areas to be accessed, or changes regarding subjects to be discussed take place during the conduct of the visit or assignments, notify your site foreign visits and assignments office. Notify that office in the event that host duties are transferred from one employee to another employee.

During the course of the visit or assignment, it may be necessary for others to escort the foreign national while he/she works or travels within your site. Escorts must:

- be familiar with the site, to include security areas;
- have full knowledge and understanding of all security plan requirements associated with the visit/assignment;
- have knowledge of the specific information or technologies to which the foreign national has been authorized access, to ensure that unauthorized access does not occur; and
- have the appropriate access authorization for escort duties, as required by the site.

i. Discuss and describe the systems in place to ensure there are no unauthorized access/unintentional disclosure of classified matter, SNM, and/or sensitive unclassified information/technology (including Cooperative Development Agreements and export control information).

The following is taken from DOE M 470.4-1 chg 1.

The basic strategies pertaining to protection are denial of access, denial of task, and containment that upon failure could evolve into recapture/recovery or pursuit strategies. Protection programs and tactical deployments designed to prevent unauthorized control of material and devices and to prevent acts of radiological, biological, chemical, and disruption of critical mission must be integrated with protection strategies. These activities could include protection layers of IDS and concentric security areas, access control measures, compartmentalization, insider protection programs, and procedural measures.

j. Discuss the counterintelligence requirements of the Unclassified Visits and Assignments of Foreign Nationals program.

This following is taken from DOE O 475.1.

Pursuant to E.O. 12333, *United States Intelligence Activities*, and DOE procedures for intelligence activities, it is DOE policy to protect programs, resources, facilities, and personnel from intelligence collection by or on behalf of international terrorists or foreign powers or entities and related threats through implementation of an effective, efficient CI program. Since the signing of Presidential Decision Directive (PDD) 61, *U.S. Department of Energy Counterintelligence Program Unclassified (U)* (February 1998), the Department has taken aggressive measures to strengthen the CI program now administered by the OCI and

the NNSA ODNCI. DOE O 475.1, *Counterintelligence Program*, reflects the current CI program scope and requirements.

The OCI Director supports UFVA activities as follows:

- Establishes and identifies CI policy and information requirements related to access by foreign nationals to DOE sites, programs, technologies, and information for inclusion in the UFVA Program.
- Provides advice to headquarters approval authorities and supports field CI officers with guidance on foreign national access issues to consider in reviews.
- Ensures that local capability and expertise is available to provide effective CI advice to local approval authorities regarding access approval requests.
- Develops and provides CI awareness modules for UFVA training.
- Coordinates the external indices check process with the appropriate U.S. government agencies.
- Documents and maintains DOE-wide information on requests for and completion of indices checks.
- Maintains separate, classified analytical databases to document foreign interaction at DOE sites.
- As a member of the Secretary's Headquarters Management Panel, reviews applications for nationals of state sponsors of terrorism visits.
- Establishes policy on CI briefings/debriefings for DOE personnel on official travel to countries where they intend to have or have had discussions with sensitive country foreign nationals regarding sensitive subjects. This would include travel known in advance to involve meetings with sensitive country foreign nationals or chance meetings where there are foreign nationals from sensitive countries in attendance.

The following is taken from DOE O 142.3 chg 1.

Access requests for nationals of state sponsors of terrorism require approval by both the site approval authority and the sponsoring HQ program office before final approval determination. Final approval authority is held by the Secretary of Energy and can only be assigned to the Under Secretary for Nuclear Security/Administrator for the NNSA, Under Secretary of Energy or Under Secretary of Energy or Under Secretary for Science.

The HQ management panel consists of the Chief Health, Safety and Security Officer; the Deputy Director, Counterintelligence Directorate; and a representative designated by the appropriate under secretary. The HQ management panel will review requests submitted by sponsoring HQ program offices and provide advisory recommendations either to the Secretary of Energy or to the appropriate under secretary for review and final approval determination.

The Office of Foreign Visits and Assignments will coordinate reviews by the HQ Offices of Health, Safety and Security; Intelligence and Counterintelligence; Defense Nuclear Nonproliferation; and any other reviews required by DOE security directives before submitting requests for review and final approval determination.

B. PHYSICAL SECURITY (PS)

Competencies and supporting knowledge and skills for section B, PS, are derived from the following DOE Orders, manuals, and guides:

- 10 CFR 860, "Trespassing on Department of Energy property"
- 10 CFR 1046, "Physical Protection of Security Interests"
- 41 CFR 101, "Federal Property Management Regulations"
- DOE M 470.4-1 chg 1, *Safeguards and Security Program Planning and Management*
- DOE M 470.4-2 chg 1, *Physical Protection*
- DOE M 470.4-6 chg 1, *Nuclear Material Control and Accountability*
- DOE M 471.1-1 chg 1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*
- DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*
- DOE O 470.3B, *Graded Security Protection (GSP) Policy*

[Note: DOE O 470.3B is a classified document. This reference guide does not contain any information from DOE O 470.3.]
[Note: DOE M 470.4-2 chg 1 has been superseded by DOE M 470.4-2A.]

16. Safeguards and security personnel with the responsibility for PS must demonstrate a working level knowledge of graded physical protection programs and site physical protection programs.

a. Describe the planning, execution, evaluation, and documentation requirements required for site physical protection programs as outlined in the SSSP. For sites not requiring an SSSP, describe the planning, execution, evaluation, and documentation requirements required for site physical protection programs as outlined in a SSP.

The following is taken from DOE M 470.4-2A.

The implementation of graded physical protection programs required by DOE M 470.4-2A must be systematically planned, executed, evaluated, and documented as described by an SSP.

- Physical protection programs must be based on the most recent GSP information and used in conjunction with local threat guidance. The GSP applies to all DOE facilities including those that do not possess classified matter or SNM.
- Departmental interests must be protected from malevolent acts such as theft, diversion, and sabotage and events such as natural disasters and civil disorder by considering site and regional threats, protection planning strategies, and protection measures.

- SNM must be protected at the higher level when roll-up to a higher category can occur within a single security area unless the facility has conducted an analysis that determined roll-up was not credible.
- Sites upgrading security measures must consider the benefits provided using security technology by conducting life-cycle cost-benefit analysis comparing the effectiveness of security technology to traditional manpower-based methodologies. However, at category I/II facilities various manpower alternatives to include security technologies must be used to allow PF personnel to concentrate on the primary mission of protecting nuclear weapons, SNM, and designated high-value targets.

b. Describe the following five elements of protection and control planning:
- **Site-specific characteristics**
- **Threat**
- **Protection strategy**
- **Planning**
- **Graded protection**

The following is taken from DOE M 470.4-1 chg 1.

Site-Specific Characteristics

Protection programs must be tailored to address specific site characteristics and requirements, current technology, ongoing programs, and operational needs to achieve acceptable protection levels that reduce risks in a cost-effective manner.

Threat

DOE O 470.3 has been superseded by DOE O 470.3B which is classified. This Order must be used with local threat guidance during the conduct of VAs for protection and control program planning. The DBT must be the baseline threat definition but local threat guidance may be used to increase the level of threat to be analyzed.

Protection Strategy

Targeted protection strategies:
- Strategies for the physical protection of SNM and vital equipment must incorporate the applicable requirements established in DOE M 470.4-2A.
- Protection strategies must be implemented as specified in the DBT. PF resources must focus on decisively defeating the terrorist threat, which is facilitated by positioning posts so there is little or no delay in responding to critical targets, eliminating posts which detract from constant readiness, and maximizing use of physical protection systems to enhance PF effectiveness. PF resources must be positioned to interdict and neutralize the adversary threat as far as possible outside the boundaries of the target location.
- Protection program elements must be designed to prevent and/or mitigate the consequences of acts of radiological, chemical, or biological sabotage that would cause unacceptable impact to national security, the environment, or the health and safety of the public or employees. Protection elements, such as active denial systems,

must be designed and deployed to minimize the need for PF recapture/recovery operations.
- Strategies for the protection and control of classified information or matter must incorporate the applicable requirements established in DOE M 470.4-4, *Information Security*.
- Security systems must be used that prevent, detect, or deter unauthorized access, modification, or loss of classified and unclassified controlled matter and its unauthorized removal from a site or facility.
- Strategies for the protection of government property not covered above must reflect a graded approach. DOE offices, facilities, and PPAs must meet or exceed GSA minimum security standards.
- Security countermeasures for explosive threats must address a range of activities including hand-carried, mailed, and vehicle-transported devices.

Planning

S&S plans must be developed for facilities with any of the following S&S interests:
- Category I quantities of SNM or credible roll-up quantities of SNM to a category I quantity
- Category II, III, or IV SNM
- Radiological, chemical, or biological sabotage threats
- Critical mission disruption threats
- Intra-/inter-site transportation of SNM
- Classified information or matter
- Facilities engaged in the protection of government property
- Facilities that the Secretary, Deputy Secretary, or under secretaries deem appropriate

Graded Protection

The Department recognizes that risks must be accepted (i.e., that actions cannot be taken to reduce the potential for or consequences of all malevolent events to zero); however, an acceptable level of risk must be determined based on evaluation of a variety of facility-specific goals and considerations. By a graded approach, the Department intends that the highest level of protection be given to security interests and activities whose loss, theft, compromise, and/or unauthorized use would seriously affect the national security, the environment, departmental programs, and/or the health and safety of the public or employees. Protection of other interests and activities must be graded accordingly.

c. Describe how the graded security protection (GSP) Policy is used in S&S program planning.

GSP policy is covered in DOE O 470.3B which is classified as Secret//RD//No Foreign (NOFORN). This reference guide does not contain any information from DOE O 470.3B.

d. Describe the principles of the VA process and how the PS program is a part of a facility's VA program.

The following is taken from DOE M 470.4-1 chg 1.

The VA program must consider other programs such as PF, MC&A, emergency operations, safety, maintenance, facility operations, PS, physical protection, and information security. The process of conducting a VA includes gathering data that describe the physical and operational characteristics of an S&S system, assigning values such as delay and detection, and analyzing the results to determine the relative effectiveness in conjunction with the adversary's capabilities as identified in the DBT and the adversary capabilities list (ACL).

The VA process includes the following:

- Assumptions and scoping agreements must be defined. All assumptions must be documented in the VA report.
- The person responsible for the conduct of VAs, hereinafter referred to as the analyst, must understand how the DBT relates to VAs. The analyst performing the VA must apply DOE HQ, regional, and local threat guidance.
  - DOE HQ threat:
    - The DBT must be used to define threat against which VA analysts evaluated the protection system.
    - The site's protective systems must be analyzed against the ACL.
  - Regional and local threats must be considered during the conduct of VAs.
- All security interests whose loss, theft, compromise, and/or unauthorized use will affect the national security and/or the health and safety of DOE and contractor employees, the public, the environment, or DOE programs are potential targets. The analyst must consider target configurations and conditions, as well as operational conditions and acquisition times.
- Modeling is used to analyze S&S programs, interests, assets, and the effectiveness of program implementation. Modeling can include computer-based tools and simulations, table-top analyses, and SME analyses. DOE M 470.4-1 chg 1, section E, appendix 3, *VA Modeling Tools*, lists those modeling tools approved by DOE. Methods to ensure that the models accurately reflect the facility posture must be part of the final VA results. The modeling process must establish critical pathways. The following must be considered:
  - Facility characterization.
  - System effectiveness models and equations must be used.
  - Response force times.
  - The P_N must be calculated using data available regarding the PF response and their ability to interrupt and neutralize an adversary.
  - Blast effect modeling must consider blast effects on barrier breaching, a force multiplier, and target buildings.

- Table-top methods used to determine system effectiveness must be documented and a means provided to allow for validation or verification.
- Radiological sabotage must be fully analyzed against the DBT and ACL.
- Chemical and biological sabotage must be analyzed against the DBT and ACL.
- The analysis must use the thresholds stated in DOE O 470.3B.
- The use of chemical and biological agents must be analyzed as a force multiplier.

- If conducted, the results of the following tests (including validation) must be considered in determining system effectiveness:
  - FoF exercises
  - LSPTs
  - ARAPTs
  - Breaching test data
  - Critical system element tests
- The results of VAs indicate P_E. The VA results must be used for determining:
  - Protection system effectiveness reporting
  - S&S upgrades
  - Manning/armament levels for the PF
  - Justifications for waivers of and exceptions to S&S policy
- VA practitioners must successfully complete VA program training within two years of appointment. This requirement can be met through the NTC.

e. Describe the method used to identify and characterize the range of potential adversary threats.

The following is taken from DOE M 470.4-1 chg 1.

Threat description—establish a graded approach to protection for category I SNM and SNM facilities with credible roll-up of SNM to a category I quantity, and facilities having radiological, biological, or chemical, sabotage event potential and facilities having disruption of critical mission sabotage event potential. Use the DBT as the baseline for threat determination, along with higher levels of threat dictated by local and regional threats, and describe the site-specific threats used as the basis for conducting VAs and for which the protection program is designed.

Threat identification—identify, describe, and prioritize targets of security interest that meet the following criteria:

- Category I quantities of SNM and the facilities with credible roll-up of SNM to a category I quantity.
- A radiological, biological, or chemical sabotage inventory that, if released, would cause an unacceptable impact on national security or the health and safety of employees, the public, or the environment.

- Critical national security facilities, and assets (as defined in the DBT), designated by the Department that would impact DOE programs supporting national defense and security.
- Those facilities possessing automated information systems that process or contain SCI, SAP, weapon data classified S/RD Sigma 1, 2, 14, and 15 or higher.
- Temporary recurring targets. When predictable programmatic operations can reasonably be expected to present temporary SNM, sabotage, or information targets such as those permanent locations previously described, these targets must be described and analyzed at the same level of detail and in the same manner as permanent locations.

f. Discuss the denial strategy used to protect S&S interests.

The following is taken from DOE M 470.4-1 chg 1.

Denial strategy implementation:

- Early warning system technologies are emplaced to detect and to assess adversary movement as far as possible from target locations.
- High mobile tactical vehicles (armored and/or unarmored) mounted with light and/or heavy weapon systems are deployed to support combat operations, conduct reconnaissance operations, control avenues of approach, maneuver to suppress and destroy hostile threats, and to provide mutual support for other tactical vehicles.
- A commander is designated for each tactical armored vehicle (for a two-person crew, usually the gunner).
- Potential target access points are covered by suppressive fire weapons.
- TRF members utilize positions of cover and maximize the element of surprise to the extent possible.
- The TRF initiates a decisive engagement with adversary forces as far as possible outside the target location.
- Once an adversary has been identified and engaged, TRF elements never lose contact.
- Adversaries are engaged while they negotiate obstacles (e.g., fences, barriers, etc.), deploy from vehicles (both airborne and ground-based), and cross open ground.
- TRF teams, using suppressive fire weapons, maneuver in force against adversaries occupying covered positions.
- The TRF has plans in place to transition quickly from defensive to offensive operations.

g. Discuss the performance testing requirements for physical protection systems.

The following is taken from DOE M 470.4-2A.

Systems and system elements are to be performance-tested at a documented frequency (see DOE M 470.4-1 chg 1). The testing program must be implemented in locally prepared planning or procedural documents.

The following is taken from DOE M 470.4-1 chg 1.

At least every 365 days, an integrated performance test encompassing all essential protection elements associated with a comprehensive site or facility threat scenario must be conducted to evaluate the overall facility S&S effectiveness.

- Those category I facilities requiring denial protection strategies must conduct integrated performance testing on a quarterly basis (at least every three months).

OR

- Those sites with multiple category I facilities requiring denial protection strategies may rotate quarterly performance testing so that at least one facility is tested on a quarterly basis (at least every three months). However, an integrated performance test for all category I facilities must occur at least once every three hundred sixty-five days.

17. Safeguards and security personnel with the responsibility for PS must demonstrate a working level knowledge of physical protection systems.

a. Describe the three primary functions of a physical protection system.

The following is taken from DOE M 470.4-2A.

The three primary functions of a physical protection system are: planning, implementing, and monitoring the application of physical protection measures. The chapters and appendices in DOE M 470.4-2A describe the procedures and management process applicable to departmental operating environments. Implementation of these procedures should be accomplished under an approved security plan, as described in DOE M 470.4-1 chg 1 that describes an integrated, performance-based approach to site security.

b. Describe the characteristics of an effective physical protection system.

The following is taken from DOE M 470.4-2A.

The characteristics of an effective physical protection system include the following components:

- Alarm stations that provide a capability for monitoring and assessing alarms and initiating responses to S&S events.
- Commercial alarm service firms must issue a current Underwriter's Laboratory (UL) certification commensurate with the contracted service and must maintain this UL certification as long as the service is provided to the facility. For the protection of classified matter UL 2050, National Industrial Security Service standard should be implemented and a certificate issued for compliance with the UL standard.
- An alarm assessment system that allows security personnel to determine rapidly whether an intrusion has taken place at a remote location. When used, assessment

systems must be configured as an element of the total IDS along with the required complementary lighting.
- Systems and system elements are to be performance-tested at a documented frequency. The testing program must be implemented in locally prepared planning or procedural documents.
- Corrective maintenance procedures for supporting security related systems and subsystems protecting category III and IV quantities of SNM, must be approved by line management and prescribed in the site's operation procedures.
- An interior IDS.

c. Describe the fundamental characteristics of exterior and interior intrusion sensors.

The following is taken from DOE M 470.4-2A.

Interior Intrusion Sensor

When used to protect either category of SNM, IDSs must be configured to
- detect unauthorized access to category III and IV quantities of SNM;
- be compatible with other interior and exterior alarm devices and systems;
- automatically activate an alarm to notify of a changed security condition;
- function effectively in all environmental conditions;
- provide alarm communication line supervision;
- provide tamper protection on all alarm devices and alarm data gathering panels;
- have a false and nuisance alarm rate as described in DOE M 470.4-2A, appendix A, chapter IX, while maintaining proper detection sensitivity; and
- report alarm conditions to a dedicated location that facilitates continuous monitoring by designated, trained PF or security personnel.

Exterior Intrusion Sensors

When used for either category of SNM, exterior IDSs must be configured to
- detect unauthorized access to category III and IV quantities of SNM;
- complement the interior IDS;
- automatically activate an alarm to notify of a changed security condition;
- function effectively in all environmental conditions;
- provide alarm communication line supervision;
- provide tamper protection on all alarm devices and alarm data gathering panels;
- have a false and nuisance alarm rate as described in DOE M 470.4-2A, appendix A, chapter IX, while maintaining proper detection sensitivity;
- report alarm conditions to a dedicated location which facilitates continuous monitoring and assessment by designated trained PF or security administrative personnel; and
- the CSA develops the false alarm rates/nuisance alarm rates standards based on site-specific systems to achieve a low as is reasonably achievable (ALARA) levels.

d. Using a list of exterior and interior sensors, describe the operating characteristics of each type of sensor.

The following is taken from DOE M 470.4-2A.

Interior IDS

Interior systems must be designed, installed, and maintained to deter adversaries from circumventing the detection system.

- Interior systems must be installed to eliminate gaps in detection coverage.
- The IDS must be tested when installed and annually (at least every twelve months) thereafter.
- If testing indicates degradation of the IDS, it must be repaired and retested.
- Interior IDSs may be used as compensatory measures for unattended entry/exit points, utility ducts, or other openings meeting the unattended openings requirements contained in DOE M 470.4-2A.

Balanced magnetic switches (BMSs) must initiate an alarm upon attempted substitution of an external magnetic field when the switch is in the normal secured position and whenever the leading edge of the door is moved 1 inch (2.5 centimeters) from the door jam.

Tests for volumetric interior IDSs must consider a range of tests, (e.g., walk tests, voltage variation, temperature and humidity, electromagnetic susceptibility, vibration, standby power, and handling shock tests). A functional test, in conformance with the manufacturer's specification, should be performed prior to acceptance of the installed system and thereafter as determined necessary by the facility. Interior IDSs must be performance-tested according to locally established procedures, (e.g., walking, running, jumping, crawling, or rolling along the path to the item being protected) at a documented frequency.

Exterior IDS

Exterior IDSs must be designed, where economically feasible, with independent redundant data communication paths for protecting DOE S&S interests. The paths must be documented in an SSP or protection procedures, consistent with DOE M 470.4-2A, table 1, *Line Supervision Protection*.

The IDS must be capable of detecting an individual crossing the detection zone by walking, crawling, jumping, running, rolling, or climbing the fence at any point in the detection zone, with a detection probability of 90 percent and confidence level of 95 percent.

- The IDS must be tested when installed and annually (at least every twelve months) thereafter to validate that it meets detection probability and confidence level requirements.
- Any time the IDS falls below the required probability of detection, the IDS must be repaired and retested.
- When calculating detection probability for multiple sensor technology systems, detection is assumed if any of the sensors/zones report an intrusion. Multiple sensor

technology systems may include taut wire, microwave, infra-red, ported coax, and laser components.

For all openings in exterior barriers, unattended gates and/or entry/exit points, culverts, and sewers, that meet the unattended opening criteria of DOE M 470.4-2A, chapter VI, intrusion detection capabilities must be as effective as the rest of the perimeter IDS.

Perimeter Alarm/Detection and Assessment systems must be

- designed to cover the entire perimeter without a gap in detection, including the sides and tops of structures situated within;
- located such that the length of each detection zone is consistent with the characteristics of the sensors used in that zone and the topography;
- designed, installed, and maintained to deter adversaries from circumventing the detection system;
- provided with an isolation zone at least 20 feet (6 meters) wide and clear of fabricated or natural objects that would interfere with operation of detection systems or the effectiveness of the assessment;
- free of wires, piping, poles, and similar objects that could be used to assist an intruder traversing the isolation zone or that could assist in the undetected ingress or egress of an adversary or matter; and
- constructed in a manner that detects and deters the use of wire, piping, poles, etc., that cannot be eliminated from the isolation zone.

Each alarm zone must be kept free of snow, ice, grass, weeds, debris, wildlife, and any other item that may degrade the effectiveness of the system. When this cannot be accomplished and detection capabilities become degraded, compensatory measures are required.

e. Describe the types of exterior and interior sensors used within DOE.

This is a performance-based KSA. The Qualifying Official will evaluate its completion.

f. Describe the components of a comprehensive entry control and contraband detection system.

The following is taken from DOE M 470.4-2A.

Entry control point systems must allow the authorized entry and exit of personnel while detecting prohibited and controlled articles. Entry control point configuration must have separate material package inspection areas/stations for inspecting personnel, packages, and hand-carried items. The following design criteria apply:

- Entry/exit point inspection monitors must be collocated with designated security posts to facilitate the initiation of a response to an alarm.
- Security posts must be designed with an unobstructed view to facilitate observation of any attempt to bypass systems.

- Security structures should consider the requirements in DOE M 470.4-2A, appendix B.
- Entrances/exits must be alarmed with intrusion detection sensors or controlled at all times to notify of unauthorized use.

g. Describe the types of access control systems used within DOE.

The following is taken from DOE 470.4-2A.

Access controls must be in place to ensure that only appropriately cleared and authorized personnel are permitted unescorted access to the LA. Access must be based on an individual's need-to-know to perform official duties, validation of the individual's security clearance, and the presentation of a DOE security badge. Access must be controlled when going from one security area into another security area with increased protection requirements. Where practical, automated access control systems should replace PF or other authorized personnel to control access into security areas.

- If automated access control equipment is used, a DOE security badge must be used to access electronically stored information relevant to the badge and badge holder.
- Entry control points for vehicle and pedestrian access to security areas must provide the same level of protection as that provided at all other points along the security perimeter.
- Entry control points must be structurally hardened to meet site-specific criteria as documented in the SSP.
- Exits from security areas must satisfy life safety requirements of National Fire Protection Association (NFPA) 101, "Life Safety Code." Some exits may be provided for emergency use only.
- Security area entrances and exits must be equipped with doors, gates, rails, or other movable barriers that direct and control the movement of personnel or vehicles through designated control points.
- Door locks and latches used on security area perimeters must meet life safety requirements of NFPA 101.
- Automated gates must be designed to allow manual operation during power outages or mechanism failures. Where automated gates are used to control vehicular access to a security area, the gates and openings must be constructed to permit operation from a monitoring/control point or from other manned security posts.
- Site-specific requirements and procedures for visitor logs must be approved by the CSA. If visitor logs are to be used at the PPA, the requirements set forth in DOE M 470.4-2A, chapter II, are to be followed.

h. Describe the purpose of access delay in a physical protection system.

The following is taken from DOE M 470.4-2A.

Mechanisms must be used to deter and delay access, removal, or unauthorized use of category I and II quantities of SNM and nuclear weapons.

- Delay mechanisms may include both passive physical barriers (e.g., walls, ceilings, floors, windows, doors, and security bars) and activated barriers (e.g., sticky foam, pop-up barriers, cold smoke, and high-intensity sound). The appropriate delay mechanisms must be used at site-specified target locations to reduce reliance on PF recapture/recovery operations.
- Active and passive denial systems will be deployed, as appropriate, to reduce reliance on recapture operations.

i. Describe the type of access delay mechanisms used within DOE.

This is a performance-based KSA. The Qualifying Official will evaluate its completion.

j. Discuss the following terms:
- **Defense-in-depth**
- **Probability of detection**
- **Delay time**
- **Active and passive barriers**
- **Complementary sensors**
- **Assessment**
- **Detection**
- **Compensatory measures**

Defense-in-Depth

The following is taken from DOE M 470.4-7 (archived).

The use of multiple, independent protection elements combined in a layered manner so that system capabilities do not depend on a single component to maintain effective protection against defined threats.

Probability of Detection

The following is taken from DOE M 470.4-7 (archived).

The likelihood of a detection element of a PS system (e.g., sensor, SPO, etc.) recognizing an external stimulus as an adversarial action within a specific zone of coverage.

Delay Time

The following is taken from DOE M 470.4-2A.

An SNM vault must be a penetration-resistant enclosure that has doors, walls, floor, and roof/ceiling designed and constructed to significantly delay penetration from forced entry and equipped with IDS devices on openings allowing access. The material thickness must be determined by the requirement for forcible entry delay times for the S&S interests stored within, but must not be less than the delay time provided by a minimum 8-inch (20.32-centimeters)-thick reinforced concrete poured in place with a twenty-eight-day compressive strength of 2,500 pounds per square inch (17,237 kilopascal).

Active and Passive Barriers

The following is taken from DOE M 470.4-7 (archived).

Delay mechanisms are employed to impede removal or unauthorized use of departmental property, such as

- Passive barriers are (e.g., walls, ceilings, floors, windows, doors, security bars), activated barriers are (e.g., sticky foam, pop-up barriers) and visual obscurants (e.g., cold smoke).
- A passive barrier is an obstruction to passage which, by its name, impedes or deters entry or exit (e.g., a wall, ceiling, floor, or fence).
- Activated barriers are dispersible materials which are activated either remotely or in response to a stimulus, and which are designed for direct interference with human sensory and/or motor processes. They include non-pyrotechnic smoke, aqueous foam, rigid foam, cold smoke, and chloracetophenon gas.

Complementary Sensors

The following is taken from the Defense Advanced Research Projects Agency, *Perimeter Security Sensor Technologies Handbook*.

When one type of sensor does not afford enough physical protection, another type of sensor is used in conjunction in order to ensure adequate protection. Complementary sensors for interior applications include BMSs, glass break detectors, and time delayed cameras. For exterior applications video motion detection is a good complement.

Assessment

The following is taken from DOE M 470.4-7 (archived).

An assessment is

- an evaluation of the effectiveness of an activity/operation or a determination of the extent of compliance with required procedures and practices;
- an evaluation of an MC&A anomaly or material discrepancy indicator;
- an appraisal of the credibility, reliability, pertinence, accuracy, or usefulness of information;
- an evaluation of a PS alarm; or
- a determination of the validity and priority of an incident.

Detection

The following is taken from DOE M 470.4-7 (archived).

Detection:

- The positive assessment that a specific object is the cause of the alarm.
- The announcement of a potential malevolent act through alarms.

Compensatory Measure

The following is taken from DOE M 470.4-7 (archived).

Compensatory measures are temporary safeguards or security activity designed to afford equivalent protection for safeguards or security interests when a protection system element has failed or new requirement or vulnerability has been identified.

k. Demonstrate the modeling of a physical protection system using an adversary sequence diagram.

This is a performance-based KSA. The Qualifying Official will evaluate its completion.

18. Safeguards and security personnel with the responsibility for PS must demonstrate a working level knowledge of the protection of nuclear weapons, components, and SNM.

a. Discuss the graded approach in relation to the protection of S&S interests.

The following is taken from DOE M 470.4-2A.

DOE M 470.4-2A establishes requirements for the physical protection of interests under DOE's purview ranging from facilities, buildings, government property, and employees to national security interests such as classified information, SNM, and nuclear weapons. A graded approach for the protection of the lowest level of government property and layered to the most critical are described in DOE M 470.4-2A and its appendices.

- Graded protection requirements for the various interests under DOE's purview may be required and based on best business practices, economic rationale, national security objectives, or other rationale.
- Not all departmental interests can be identified within DOE M 470.4-2A. Therefore, DOE line management must consider departmental interests (i.e., all non-national security interests) and develop protection requirements tailored to that particular interest using graded protection measures.
- To effect DOE P 470.1, *Integrated Safeguards and Security Management Policy (ISSM)*, dated 5-8-01, sites must integrate PS protection into DOE operations and according to sound risk management practices. The ISSM is the department's philosophical approach to the management of the S&S Program. A principal objective to ISSM is to integrate S&S into management-based decisions so missions may be accomplished without security events such as interruption, disruption, or compromise.
- Physical protection must be integrated with other S&S programs such as PP&M, PF, information security, personnel security, and nuclear MC&A.
- The activities and requirements outside of the S&S Program in the weapons surety, foreign visits and assignments, safety, emergency management, CS, intelligence, and CI programs must also be considered in the implementation of DOE M 470.4-2A.

b. Describe the protection for Category I and II SNM, such as denial and containment, and recapture, recovery, and/or pursuit.

The following is taken from DOE M 5632.1C-1 (archived).

Strategies for the physical protection of SNM and vital equipment shall incorporate the applicable requirements established in DOE M 5632.1C-1, *Manual for Protection and Control of Safeguards and Security Interests* (archived), chapter II. Protection strategy may be graduated to address varying circumstances and may range from denial to containment to recapture/recovery to pursuit.

- A denial strategy shall be used for the protection of a S&S interest (e.g., category IA SNM, certain radiological sabotage targets) where unauthorized access presents an unacceptable risk. Programs shall be designed to prevent unauthorized control; (i.e., an unauthorized opportunity to initiate or credibly threaten to initiate a nuclear dispersal or detonation, or to use available nuclear materials for onsite assembly of an improvised nuclear device).
- A containment strategy shall be used to prevent the unauthorized removal of category II or greater SNM.
- Should denial and/or containment referenced in DOE M 5632.1C-1, chapter I, 3.a.(1) and (2) fail, a recapture/recovery or pursuit strategy would then be required. Forces capable of rapid reaction are vital to the implementation of recapture or recovery contingencies.
- Programs must be designed to mitigate the consequences of acts of radiological/toxicological sabotage that would cause unacceptable impact to national security or pose significant dangers to the health and safety of employees, the public, or the environment.

Strategies for the protection and control of classified matter shall incorporate the applicable requirements established in DOE M 5632.1C-1, chapter III. In addressing the threat to the Department's information assets, emphasis must be placed on security systems that will detect or deter unauthorized disclosure or modification or the loss of availability of classified and sensitive, but unclassified, information and its unauthorized removal from a site or facility.

Security countermeasures to address bombing shall consider a range of activities from hand-carried, mailed, and vehicle-transported devices.

Programs shall be designed to prevent radiological/toxicological sabotage acts that would cause unacceptable impact to national security or pose significant dangers to the health and safety of employees, the public, or the environment, and/or to mitigate the consequences of such acts that might occur. S&S systems and critical systems elements shall be performance-tested to ascertain their effectiveness in providing countermeasures to address DBTs.

c. Describe the physical protection for each category of SNM considering the following factors:
- **Quantities**
- **Chemical forms**
- **Isotopic composition purities (ease of separation, accessibility, concealment, and portability)**
- **Radioactivity**
- **Self-protecting features**

[Note: The term vault-type room (VTR) has been replaced with the term closed areas (CAs). Ref: NAP-70.4.]

The following is taken from DOE M 470.4-2A.

The priority of protection measures must be designed to prevent malevolent acts such as theft, diversion, and radiological sabotage and to respond to adverse conditions such as emergencies caused by acts of nature.

- A facility must not possess, receive, process, transport or store SNM until that facility has been cleared.
- Physical protection for each category of SNM must consider the following factors: quantities; chemical forms; isotopic composition purities: ease of separation, accessibility, concealment, and portability; radioactivity; and self-protecting features.
- The protection of nuclear material production, reactors, and fuel must be commensurate with the category of SNM.
- SNM, parts, or explosives that are classified must receive the physical protection required by the higher level of classification or category of SNM, whichever is the more stringent.

Category I quantities of SNM, the following apply:

- Category I quantities of SNM must be located within an MAA inside a PA. Any MAA containing unattended category quantities of SNM must be equipped with an IDS or detection must be provided by PF.
- Category I, attractiveness level A SNM must be stored in a vault. Storage facilities constructed after July 15, 1994 for category I, attractiveness level A SNM must be underground or below grade.
- Category I, attractiveness level B SNM must be stored in a vault or provided enhanced protection that exceeds closed area (CA) storage.
- At a minimum category I, attractiveness level C SNM must be stored in a CA.

Category II quantities of SNM, the following apply:

- Category II quantities of SNM must be located within a PA and under material surveillance procedures.
- Category II quantities of SNM must be stored in a vault or VTR located within a PA.

Category III quantities of SNM, the following apply:

- Category III quantities of SNM must be used or processed in an access-controlled security area within at least an LA and according to local security procedures approved by the DOE CSA.
- Category III quantities of SNM must be stored within a locked security container or room, either of which must be located within at least an LA. The container or room must be under the protection of an IDS or PF patrol physical check at least every eight hours.

Category IV quantities of SNM, the following apply:

- Category IV quantities of SNM must be used or processed within at least a PPA and according to local security procedures approved by the DOE CSA.
- Category IV quantities of SNM must be stored in a locked area within at least a PPA, and procedures must be documented in an approved SSP.

d. Discuss the following as they relate to the integrated physical protection of nuclear weapons and Category I and II quantities of SNM:

- **Intrusion detection systems**
- **Delay mechanisms**
- **PF**
- **Storage controls**

The following is taken from DOE M 470.4-2A.

Intrusion Detection

Category I and II quantities of SNM must be protected by an integrated physical protection system using PF, barriers, and intrusion detection and assessment systems (IDAS). IDAS must be designed with independent, redundant data communication lines, intrusion detection and assessment must be immediate, and the video signal must be protected based on the classification level. Video signal would include video signal encryption for conditions wherein video coverage cannot be masked from viewing classified matter. Exterior IDAS are designed to detect unauthorized entry into security areas.

Delay Mechanisms

Mechanisms must be used to deter and delay access, removal, or unauthorized use of category I and II quantities of SNM and nuclear weapons.

- Delay mechanisms may include both passive physical barriers (e.g., walls, ceilings, floors, windows, doors, and security bars) and activated barriers (e.g., sticky foam, pop-up barriers, and cold smoke and high-intensity sound). The appropriate delay mechanisms must be used at site-specified target locations to reduce reliance on PF recapture/recovery operations.
- Active and passive denial systems will be deployed, as appropriate, to reduce reliance on recapture operations.

PF

PF Tracking Systems. Systems capable of tracking and displaying the live movements and state-of-health of PF may be used to improve the situational awareness of PF commanders. Data associated with these systems are typically transmitted by radio frequency so the following limitations apply:

- Classified information may not be transmitted by the wireless communications associated with tracking systems.
- PF tracking systems used at sites with category I quantities of SNM must be evaluated prior to implementation by the CSA. The evaluation is to determine if the high system effectiveness rating, as described in DOE M 470.4-1 chg 1, would be degraded, if compromised unless encrypted

Storage

Category I quantities of SNM must be stored within a material access area (MAA).

- Category I, attractiveness level A SNM must be stored in a vault. Storage facilities constructed after July 15, 1994 for category I, attractiveness level A SNM must be underground or below grade.
- Category I, attractiveness level B SNM must be stored in a vault or provided enhanced protection that exceeds VTR storage (e.g., collocated with a PF response station and/or activated barriers).
- At a minimum, category I, attractiveness level C SNM must be stored in a VTR.

Category II quantities of SNM must be stored in a vault or VTR located within a PA.

e. Discuss the programs to mitigate radiological/toxicological sabotage.

The following is taken from DOE M 470.4-2A.

Radiological, chemical, or biological sabotage targets must be provided protection as determined by vulnerability analysis. Select biological agents and toxins are also considered DOE interests. Protection of these select biological agents and toxins are governed by 7 CFR 331, "Possession, Use, and Transfer of Select Agents and Toxins"; 9 CFR 121, "Possession, Use, and Transfer of Select Agents and Toxins"; 9 CFR 122, "Organisms and Vectors"; and 42 CFR 73, "Select Agents and Toxins." Protection of chemical facilities/activities which are considered to present a high risk are governed by 6 CFR 27, "Chemical Facility Anti-Terrorism Standards"; Final Rule.

- Depending on the interest, protection may be required based on best business practices, economic rationale, national security objectives or other rationale.
- DOE line management considers the various departmental interests and their attractiveness to theft, diversion, or sabotage and develop protection requirements using graded protection fundamentals.
- Physical protection strategies must be developed, documented, and implemented consistent with the GSP, formerly the DBT, and national policy to protect against radiological, chemical, or biological sabotage.

f. Describe access procedures to storage repositories.

The following is taken from DOE M 470.4-2A.

Access to vaults and CAs must be strictly controlled and based on an appropriate security clearance and need-to-know.

- Persons without need-to-know and the appropriate security clearance must be escorted at all times.
- Protective measures to mask classified matter must be used before visitors or cleared persons without need-to-know receive access.
- Means of controlling access must be documented in an SSP.
- Access controls at vaults and CAs must provide logging or recording of all personnel entries and exits including visitors. Logged or recorded entries must include the identification/name and date/time of entry and exit of the individual and the escort as required.
    - In vaults and CAs where entering personnel are restricted from access (e.g., a foyer) to SNM or classified matter, logging entry and exit is not required.
    - The CSA may waive the requirement for repeated logging for personnel whose offices are located within the boundary of the vaults and CAs. Initial daily entry and final daily exit logging are required.

g. Describe procedures to prevent and detect unauthorized access to a storage repository.

The following is taken from DOE M 470.4-4A.

Control systems must be established and used to prevent unauthorized access to or removal of classified information. Accountability systems must provide a system of procedures that provide an audit trail. Accountability applies regardless of the physical form of the matter (e.g., electronic, paper, or parts).

Classified matter must be stored under conditions designed to deter and detect unauthorized access to the matter, to include securing it in approved equipment or facilities whenever it is not under the direct control of an authorized person. Non-conforming storage may only be used for classified matter that cannot be protected by the established standards and requirements due to its size, nature, operational necessity, or other factors. In these exceptional cases, non-conforming storage that deters and detects unauthorized access to the classified matter may be used for storing classified matter.

h. Describe escort responsibilities when SNM is in transit.

The following is taken from DOE M 5632.1C-1 (archived).

Escort responsibilities for SNM in transit are:

- Shipment escorts shall maintain continuous communication capability with a communications center through use of transportation command (TRANSCOM) as the

primary means of communication. In the event of problems with TRANSCOM, telephonic contact at 2-hour intervals will be employed to advise of the status of the shipment for road and rail shipments and for sea shipments while shipment vessels are docked at U.S. ports.

- Shipments by highway—escort has the capability of communicating with the carrier's communications center and/or another designated communications center, and local law enforcement agencies, through the use of
  - citizens band radio
  - mobile telephone or other equivalent means of communication
- Shipments by railroad:
  - A railroad employee shall be assigned the duties of an escort. This employee will be stationed at a location on the train that will permit observation of the shipment car while in motion.
  - The escort, through the conductor, has the capability of communicating with the railroad communications center and local law enforcement agencies through the use of an on-board radiotelephone or other equivalent means of communication, which must be available on the train.
  - When the train is stopped en route on the mainline or on a siding, escorts will follow standard emergency response procedures of the railroad designed to deter trespassers, to protect railroad property, and to provide physical protection of the shipment for which the railroad is responsible as a bailee. Instructions or assistance will be requested from the communications center as required. Arrangements for such assistance should be planned and coordinated sufficiently in advance of a shipment so as to ensure maximum protection levels from this resource.
  - When a shipment car is stopped in a railroad yard awaiting classification and/or interchange, the responsibility for visual surveillance passes to special agents and/or yard watchmen responsible for yard security that can provide physical protection of the shipment car.
- Escorts, truck drivers, train crews, and ships' officers responsible for shipments of unclassified irradiated reactor fuel via commercial carriers shall be specifically trained in appropriate requirements prior to being authorized to perform such duties.

i. Discuss the protection standards for Category I thru IV SNM.

The following is taken from DOE M 470.4-2A.

Category I, II, III, and IV quantities of SNM must have the protection measures designed to prevent malevolent acts such as theft, diversion, and radiological sabotage and to respond to adverse conditions such as emergencies caused by acts of nature.

The Office of Secure Transportation (OST) is responsible for the promulgation of specific internal guidance governing the protection afforded all DOE matter entrusted to the OST for

transport by surface and air. Transportation of SNM, whether onsite or by OST, must be provided protection equivalent to that provided by fixed sites for the same material.

- A facility must not possess, receive, process, transport, or store nuclear weapons or SNM until that facility has been cleared.
- An integrated system of positive measures must be developed and implemented to protect category I and II quantities of SNM and nuclear weapons. Protection measures must address physical protection strategies of denial and containment as well as recapture, recovery, and/or pursuit.
- Physical protection for each category of SNM must consider the following factors: quantities; chemical forms; isotopic composition purities: ease of separation, accessibility, concealment, and portability; radioactivity; and self-protecting features.
- The protection of nuclear material production, reactors, and fuel must be commensurate with the category of SNM.
- SNM, parts, explosives, or munitions that are classified must receive the physical protection required by the highest level of classification or category of SNM, whichever is the more stringent.

19. Safeguards and security personnel with the responsibility for PS must demonstrate a working level knowledge of protection of classified information and matter.

a. Describe the methods for protection and control of classified matter.

The following is taken from DOE M 470.4-4A.

Protection and control requirements include the following:

- Prior to classification review, matter that may be classified must be protected at the highest potential classification level and category. The originator is responsible for obtaining a classification review by a derivative or original classifier if there are any questions regarding the classification of any draft document or working paper.
- When information is prepared on classified information systems, the hard-copy output (which includes paper, microfiche, film, and other media) must be marked either
  - with the appropriate markings for the classification of the information as determined by a derivative classifier according to a classification review of the actual output;
  - as a working paper or electronic medium to the accreditation level and category of the information system; or
  - according to the marking requirements for the appropriate classification of information that has been generated by a program verified and formally approved by the designated approving authority (DAA) to produce consistent results. The following factors must be satisfied when exercising this option:

    - The output that will be produced must be fully defined and documented. The DAA must formally approve this documentation and must ensure that any

subsequent output marked according to this option completely matches the planned and actual output for which the classification officer determined the classification level (and category if RD or FRD).
    - The classification officer must review the fully defined output and must determine the correct classification level (and category if RD or FRD) for the information contained in the output.
    - All output must be marked with the correct classification level (and category if RD or FRD) as determined by the classification officer.
- When matter must be sent outside the office of origin for a classification review and determination, it must be marked "DRAFT—Not Reviewed for Classification." To preclude marking every page of a document being transmitted for classification review, it should have a "Document Undergoing Classification Review" cover sheet that is marked with the highest level and most restrictive category of information the originator believes is contained in the document.
- Access to classified matter in an emergency involving an imminent threat (explosion, fire, etc.) to life or defense of the homeland may be provided to individuals who are not otherwise routinely eligible for access to classified matter. If an emergency is life-threatening, the health and safety of individuals takes precedence over the need to protect classified matter from disclosure. Examples of such release include providing law enforcement personnel with classified information concerning an improvised nuclear device found in a public place, sharing a classified DOE evaluation of the viability of a nuclear threat message with local emergency response personnel, or providing an attending physician with classified details about nuclear materials at a site to assist in the emergency treatment of a patient.

b. Describe the classification levels and appropriate control of classified matter at each level. [Note: The term vault-type room (VTR) has been replaced with the term closed areas (CAs). Ref: NAP-70.4.]

The following is taken from DOE M 471.2-1B (archived).

Top Secret (TS) Matter

TS matter may be stored in one of the following ways:

- In a locked, GSA-approved security container with one of the following supplemental controls:
    - Under intrusion detection alarm protection with PF response within 15 minutes of annunciation of the alarm.
    - PF, with inspections on a two-hour basis.
    - Security container equipped with a lock meeting Federal specification FF-L-2740, *Federal Specifications, Locks, Combinations*, only if the container is located in an LA, PA, MAA, or Exclusion access area.
    - Within an LA, PA, MAA, or Exclusion access area with random PF patrols at least once every eight hours during nonworking hours. Inspect at least 25 percent

of the containers once every twenty-four hours at facilities with large number of security containers.

- In a vault meeting the criteria established in DOE M 5632.1C-1 chg 1 (archived), and approved by the cognizant DOE element. The vault shall be equipped with intrusion detection protection with PF response within fifteen minutes of alarm annunciation.
- In a CA meeting the criteria established in DOE M 5632.1C-1 chg 1 (archived) and approved by the cognizant DOE element. The CA shall be under intrusion detection alarm protection with PF response within fifteen minutes of alarm annunciation. The CA shall be located within an LA, PA, MAA, or Exclusion access area.
- In a CA meeting the criteria established in DOE M 5632.1C-1 chg 1 (archived) and approved by the cognizant DOE element. If located outside of an LA, PA, MAA, or Exclusion access area, the CA shall be under intrusion detection alarm protection with PF response within five minutes of alarm annunciation.

Secret (S) Matter

S matter shall be stored in a manner authorized for TS matter or in one of the following ways:

- In a locked GSA-approved security container.
- In a vault meeting the criteria established in DOE M 5632.1C-1 chg 1 (archived) and approved by the cognizant DOE element. The vault shall be equipped with intrusion detection alarm protection with PF response within thirty minutes of alarm annunciation.
- In a CA meeting the criteria in DOE M 5632.1C-1 chg 1 (archived) and approved by the cognizant DOE element. The CAs shall be under intrusion detection alarm protection with PF response within thirty minutes of alarm annunciation. The CAs shall be located within an LA, PA, MAA, or Exclusion access area.
- In a CA meeting the criteria in DOE M 5632.1C-1 chg 1 (archived) and approved by the cognizant DOE element. If located outside an LA, PA, MAA, or Exclusion access area, the CAs shall be under intrusion detection alarm protection with PF response within fifteen minutes of alarm annunciation.
- In steel filing cabinets not meeting GSA requirements (such containers approved for use prior to July 15, 2004 may continue to be used until October 1, 2012) shall be equipped with three-position, dial-type, and built-in changeable combination locks. The cabinet must be within an LA, PA, MAA, or Exclusion access area. In addition, one of the following supplementary controls is required:
  - Intrusion detection alarm protection with PF response within 30 minutes of alarm annunciation, or
  - Inspection of the container every four hours by PF

Confidential (C) Matter

C matter shall be stored in a manner authorized for Secret matter or in a GSA-approved security container.

c. Discuss access controls, such as need-to-know, that must be established to detect and deter unauthorized access to classified matter.

The following is taken from DOE M 470.4-4A.

To establish required controls based on classification level (TS, S, or C) and category (RD, FRD), or national security information (NSI) or special handling instructions or caveats, the following is required:

- Classified matter that is generated, received, transmitted, used, stored, reproduced, permanently placed (buried according to the requirements of DOE M 470.4-4A), or destroyed must be protected and controlled commensurate with classification level, category (if RD or FRD), and caveats (if applicable). All pertinent attributes must be used to determine the degree of protection and control required to prevent unauthorized access to classified matter.
- Classified information must only be processed on information systems that have received authority to operate according to DOE Office of the Chief Information Officer (CIO) directives that establish requirements for national security systems.
- Audit trails must be implemented for all accountable classified matter.
- Buildings and rooms containing classified matter must be configured with security measures, which prevent unauthorized persons from gaining access to classified matter; specifically, security measures that prevent unauthorized physical, visual, and aural access.
- S matter that cannot be processed, handled, and/or stored within an LA or higher must be maintained in an accountability system as described in DOE M 470.4-4A, chapter II.
- Need-to-know controls, appropriate PS, and access control measures must be applied to each area or building within a security area where classified matter is processed, handled, or stored to detect unauthorized access.
- Retention requirements—all records associated with the protection and control of classified matter must be maintained according to the most current National Archives Records Administration GRS 18.
- Reporting requirements—report according to the incident reporting instructions contained in DOE M 470.4-1 chg 1.

d. Describe access procedures to storage repositories.

This information is available in DOE M 471.2-3B, *Special Access Program Policies, Responsibilities, and Procedures*, which is classified as "Official Use Only."

e. Describe procedures to prevent and detect unauthorized access to a storage repository.

This information is available in DOE M 471.2-3B which is classified as "Official Use Only."

The following is taken from DOE M 470.4-2 chg 1 (archived).

Controls for storage must:

- be documented;
- ensure that only authorized personnel have access to the storage repositories;
- detect unauthorized access;
- authenticate and document SNM movement into, or out of, storage location;
- include procedures for investigating and reporting abnormal conditions;
- provide a record system to document ingress and egress; and
- define procedures for conducting daily administrative checks.

f. Describe the level of protection for Sensitive Compartmental Information Facilities (SCIF).

SCIFs are covered in DOE M 471.2-3B which is classified as "Official Use Only."

The following is taken from Director of Central Intelligence Directive (DCID) 6/9, *Physical Security Standards for Sensitive Compartmental Information Facilities*.

A SCIF is an accredited area, room, group of rooms, buildings, or installation where SCI may be stored, used, discussed, and/or electronically processed. SCIFs will be afforded personnel access control to preclude entry by unauthorized personnel. Non-SCI indoctrinated personnel entering a SCIF must be continuously escorted by an indoctrinated employee who is familiar with the security procedures of that SCIF. The PS protection for a SCIF is intended to prevent as well as detect visual, acoustical, technical, and physical access by unauthorized persons. PS criteria are governed by whether the SCIF is in the United States or not, according to the following conditions: closed storage, open storage, continuous operations, or secure working area.

g. Describe the requirements of a Technical Surveillance Countermeasure Program.

Technical surveillance countermeasure program (TSCP) requirements are covered in DOE M 470.4-4A, section D, which is classified as "Official Use Only."

The following is taken from the DOE Headquarters Security Quick Reference Book.

The objective of the TSCP is to detect and/or deter a wide variety of technologies and techniques that can be used to obtain unauthorized access to classified and sensitive information. The HQ TSCP provides expert technical and analytical capabilities to detect, nullify, and isolate electronic eavesdropping devices, technical surveillance penetrations, technical surveillance hazards, PS weaknesses, and technical education awareness information, within DOE HQ's area of operations.

20. Safeguards and security personnel with the responsibility for PS must demonstrate a working level knowledge of radiological, chemical, and biological sabotage protection programs.

a. Describe the site/facility requirements for S&S functions for radiological, chemical, or biological sabotage protection to be coordinated and integrated into its emergency management plan and radiation protection program.

The following is taken from DOE M 470.4-2 chg 1 (archived).

The physical protection against radiological, chemical, or biological sabotage must adhere to DOE O 470.3B.

- The site/facility must ensure that S&S functions for radiological, chemical, or biological sabotage protection are coordinated and integrated into its emergency management plan and radiation protection program.
- Radiological, chemical, or biological sabotage targets must be provided protection as determined by vulnerability analyses.

b. Discuss the physical protection strategies that must be developed, documented, and implemented consistent with the GSP to protect radiological, chemical, or biological sabotage targets.

The following is taken from DOE M 470.4-2 chg 1 (archived).

Physical protection strategies must be developed, documented, and implemented consistent with the DBT to protect radiological, chemical, or biological sabotage targets.

- Radiological—targets must be protected in a graded manner to protect S&S interests and to mitigate consequences of a radiological sabotage event.
- Chemical—targets must be protected to protect S&S interests and to mitigate consequences of a chemical sabotage event.
- Biological—targets must be protected to protect S&S interests and mitigate consequences of a biological sabotage event.

c. Discuss the following prevention and mitigation measures that must be based on the results of the radiological, chemical, or biological sabotage analysis:

- **S&S features to detect or delay adversary actions**
- **Additional controls or equipment that would prevent a sabotage release scenario**
- **Event-mitigating actions such as establishing shelters, emergency notifications/evacuations, reducing and/or removing inventory quantities, or changing storage locations**

The following is taken from DOE M 470.4-2 chg 1 (archived).

The implementation of the following prevention and mitigation measures must be based on the results of the radiological, chemical, or biological sabotage analysis:

- S&S features to detect or delay adversary actions (i.e., access and materials controls, surveillance, additional barriers/alarms, and entry/exit inspections)
- Additional controls or equipment that would prevent a sabotage release scenario (e.g., providing automatic shutdown if components fail, adding backup systems, or establishing security areas)
- Event-mitigating actions such as establishing shelters, emergency notification/evacuations, reducing and/or removing inventory quantities, or changing storage locations

21. Safeguards and security personnel with the responsibility for PS must demonstrate a working level knowledge of security areas.

a. Describe the level of protection, access requirements, storage requirements, and alarm response requirements given to the following types of concentric security areas and the assets they protect:
- **Property protection areas**
- **Limited area**
- **Exclusion area**
- **Protected area**
- **Vital areas**
- **Material access areas (MAA)**

Property Protection Areas (PPAs)

The following is taken from DOE M 470.4-2A.

Level of protection—PPAs are security areas that are established to protect employees and government buildings, facilities, and property. The requirements for PPAs must be configured to protect government-owned property and equipment against damage, destruction, or theft and must provide a means to control public access. Protection may include physical barriers, access control systems, biometric systems, protective personnel or persons assigned administrative or other authorized security duties, IDSs, locks and keys, etc. The CSA must designate, describe, and document PPA protection measures within their SSP.

Access requirements—access controls must be implemented to protect employees, property, and facilities. Security requirements for personnel and vehicles entering the PPA must be established by the CSA. Procedures for the processing of visitors, including foreign nationals must be approved by the CSA and documented in the SSP (see DOE M 470.4-2A, attachment 2).

Storage requirements—category IV SNM must be stored in a locked area within at least a PPA, and procedures must be documented in an approved SSP or SSSP.

Alarm response requirements—if used, security requirements for intrusion detection, including long-range detection technologies, for the PPA must be established by the CSA.

Limited Areas (LAs)

The following is taken from DOE M 470.4-2A.

Protection level—LAs are security areas designated for the protection of classified matter and category III and higher quantities of SNM and to serve as a concentric layer of protection. LA boundaries are defined by physical barriers encompassing the designated space and access controls to ensure that only authorized personnel are allowed to enter the LA.

Access requirements—the identity and clearance level of each person seeking entry to an LA must be validated by PF, or other appropriately authorized personnel, or by an automated system and documented in the SSP.

- If automated access control equipment is used, a DOE security badge must be used to access the LA.
- Entry control points for vehicle and pedestrian access to LA must provide the same level of protection as that provided at all other points along the security perimeter.
- Exits from LAs must satisfy life safety requirements of NFPA 101. Some exits may be provided for emergency use only.
    - Security area entrances and exits must be equipped with doors, gates, rails, or other movable barriers that direct and control the movement of personnel or vehicles through designated control points.
    - Automated gates must be designed to allow manual operation during power outages or mechanism failures.
    - Site-specific requirements and procedures for receiving visitors must be developed and approved by the CSA.
    - Information from visitor logs must be retained according to local records management procedures.

Personnel access—individuals without a security clearance must be escorted by an authorized person who is to ensure measures are taken to prevent a compromise of classified matter. Validations must occur at entry control points of LAs.

- The identity and security clearance held by each person seeking entry must be validated by appropriately authorized personnel, automated systems, or other means documented in the SSP.
- Where practicable, PF personnel will not be used to control access to LAs.

Automated access control systems may be used if the following requirements are met:

- Automated access controls must verify that the DOE security badge is valid (i.e., that the badge data read by the system match the data assigned to the badge holder).
- The barrier must be resistant to bypass. The unattended entry control point should have closed-circuit television system coverage.
- Automated control system alarms (e.g., annunciation of a door alarm, duress alarm, tamper alarm, or anti-passback indication feature) must be treated as an intrusion alarm for the area being protected.

- Personnel or other protective measures are required to protect card reader access transactions, display (e.g., badge-encoded data), and keypad devices. The process of inputting, storing, displaying, or recording verification data must ensure that the data are protected according to the SSP.
- The system must record all attempts at access to include unsuccessful, unauthorized, and authorized.
- Door locks opened by badge readers must be designed to relock immediately after the door has closed.
- Transmission lines that carry security clearance and personal identification or verification data between devices/equipment must be protected according to the SSP.
- Records reflecting active assignments of DOE security badges, security clearance, and similar system-related records must be maintained.
- Badge reader boxes, control lines, and junction boxes must have line supervision or tamper indication or be equipped with tamper-resistant devices.
- Uninterrupted power supply or compensatory measures must be provided at installations where continuous operation is required.

Vehicle access:

- Approval for non-government vehicles, which includes privately owned, to access LAs must be documented in the SSP.
- Government-owned or –leased vehicles may be admitted only when on official business and only when operated by properly cleared and authorized drivers.
- The SSP must identify procedures for inspection of, and access by, service and delivery vehicles.
- All personnel within a vehicle are required to produce DOE security badges when accessing an LA and comply with individual LA procedures.
- When a remote automated access control system is used for vehicle access control, it must verify that the operator or the escort has a valid DOE security badge (e.g., the badge data read by the system must match the data assigned to the badge holder).

Storage requirements—category III quantities of SNM must be stored within a locked security container or room, either of which must be located within at least an LA.

Alarm requirements—the category III container or room must be under protection of an IDS or PF patrol physical check at least every 8 hours.

Exclusion Area (EA)

The following is taken from DOE M 470.4-2A.

Protection level—EAs are established to protect classified matter where an individual's mere presence may result in access to classified matter. The boundaries of EAs must be encompassed by physical barriers and be located within the minimum of an LA or receive approval of the CSA for those EAs not within a minimum of an LA.

Access control requirements—in addition to the requirements for an LA the following requirements apply to access an EA:

- Individuals permitted unescorted access must have the appropriate access authorizations and a need-to-know consistent with the classified matter to which they have access by virtue of their presence in the EA.
- Individuals without the appropriate security clearance and need-to-know must be escorted by a knowledgeable individual who must ensure measures are taken to prevent compromise of classified matter.
- Visitor logs must be used for EAs. The requirements cited in DOE M 470.4-2A, chapter II, paragraph 3.f, should be considered when establishing a visitor log process.

Storage requirements—category I, attractiveness level C, SNM can be stored in an EA as it requires a CA.

Alarm response requirements—intrusion detection:

- Unauthorized entry into the EA must be detected.
- When the EA is unoccupied, and classified matter is not secured in a security container, then the EA must at minimum, meet the requirements of a CA or an appropriate level of protection as determined by the CSA.

Protected Area (PA)

The following is taken from DOE M 470.4-A.

Protection level requirements—PAs are security areas typically located within an LA that are established to protect category II or greater quantities of SNM and may also contain classified matter. The PA provides concentric layers of security for the MAA. PAs must be encompassed by physical barriers that identify the boundaries, surrounded by a perimeter intrusion detection and assessment system (PIDAS), and equipped with access controls that ensure only authorized personnel are allowed to enter and exit.

Access requirements:
When the personal information number (PIN) or biometric system is either not working or not implemented at security areas requiring measures in addition to access control, PF or other trained security personnel must perform the access control requirements as documented in the SSP.

Personnel access control:

- Unescorted access must be controlled to limit entry to individuals with an L or Q security clearance.
- Visitor logs must be used for Pas.
- Validation of the security clearance must occur at PA entry control points.
    - The identity and security clearance of each person seeking entry must be validated by armed PF personnel, or

- If PA access is controlled by an unattended automated access control system, the system must verify the following:

    - A valid DOE security badge
    - Valid security clearance, and
    - Valid PIN, or
    - Valid biometric

Vehicle access controls:

- Private vehicles are prohibited.
- Government-owned or –leased vehicles or delivery vehicles may be admitted only when on official business and only when operated by properly cleared and authorized drivers or when drivers are escorted by properly cleared, authorized personnel.
- Vendor vehicles are prohibited unless the vehicles and drivers have been subjected to a thorough inspection/investigation and been given access approval by the DOE CSA. As an alternative, provisions must be established for using trained escorts.

Storage requirements—category II quantities of SNM must be located in a vault or CA located within a PA.

Alarm requirements—a PA must be encompassed by a PIDAS. The PIDAS must be monitored in a continuously manned CAS and an SAS. Specific requirements for PIDAS are listed in DOE M 470.4-2 chg 1, chapter VII.

Vital Areas

The following is taken from DOE M 470.4-2 chg 1 (archived).

Protection level requirements—vital areas are separate areas that contain vital equipment within PAs. Boundaries must conform to the layered protection concept, with a separate vital area perimeter located within a PA.

Access requirements—the perimeter must be monitored to deter and detect unauthorized entry attempts. All requirements for personnel and vehicle access control that apply to PAs, apply to vital areas.

Storage requirements—same requirements as PAs.

Alarm requirements—vital equipment must be protected with IDS. Exits must be alarmed or controlled at all times and PF response time to an intrusion alarm must be less than the delay time that can be demonstrated from the time an alarm is activated at the PA boundary to task completion.

Material Access Area (MAA)

The following is taken from DOE M 470.4-2A.

Protection level requirements—MAAs are security areas used to protect category I quantities of SNM. MAAs must have defined boundaries with barriers that provide sufficient delay time to impede, control, or deter unauthorized access. In addition to requirements for a PA the following apply to an MAA.

- MAAs must be located within a PA, but must have distinct boundaries. Multiple MAAs may exist within a single PA; however, an MAA cannot cross a PA boundary.
- While an MAA is required for the protection of category I quantities of SNM, classified matter may exist within an MAA. In such instances, the classified matter must be stored according to the requirements in DOE M 470.4-4A.

Access requirements—access control must be administered by armed PF personnel and/or automated access control systems.

- Access must be controlled to limit entry to individuals with a Q security clearance and who have been authorized for entry consistent with need-to-know and operations.
- Individuals without appropriate security clearance must be escorted.
  - The CSA must establish escort-to-visitor ratios for the MAA.
  - The escort must ensure measures are taken to prevent compromise of classified matter or access to SNM.
- S&S interests, not in approved storage within an MAA, must be controlled by the custodian or authorized user.
- Validation of security clearance must occur at MAA entry control points.
  - If MAA access is controlled by an unattended automated access control system, the system must verify
    - a valid DOE security badge
    - valid security clearance
    - valid PIN
    - valid biometric template
  - The identity and security clearance of each person seeking entry may be validated by armed PF personnel or biometrics.
- Site-specific requirements and procedures for visitors must be developed and approved by DOE line management. The procedures must provide for the information described in DOE M 470.4-2A, chapter II and attachment 2.

Security requirements for entry/exit inspections must be established by DOE line management and documented in the SSP.

- A separate physical or electronic inspection of each vehicle, person, package, and container must be conducted at all MAA exit points.
- Metal detectors used for MAA entry inspection must detect the test weapons listed in DOE M 470.4-2A, chapter V.

Storage requirements—the same as category I, attractiveness level A, SNM. SNM must be stored in a vault. Storage facilities constructed after 7/15/94 for category I, attractiveness level A, SNM must be underground or below grade.

Alarm requirements—doors at entry control points such as transfer locations must be alarmed, and the alarms must communicate with the CAS/SAS when an unauthorized exit occurs. PF response time to an intrusion alarm must be less than the delay time that can be demonstrated from the time an alarm is activated at the PA boundary to task completion. Penetrations in the floors, walls, or ceilings for piping, heating, venting, air conditioning, or other support systems must not create accessible paths that could facilitate the removal or diversion of S&S interests. Exits designated for emergency evacuation must be alarmed with IDS or controlled at all times. Active and passive denial systems will be deployed, as appropriate, to reduce reliance on recapture operations.

b. Discuss the specific access requirements for the following types of special designated security areas as applicable for your site:
- **Special access programs**
- **Alarm areas**
- **Sensitive compartmental information facilities**
- **Other designated security alarm stations**
- **Secure communication centers and automated information system centers**

This is a performance-based KSA. The Qualifying Official will evaluate its completion.

c. Discuss methods to detect, assess, deter, and prevent unauthorized access to security areas.

The following is taken from DOE M 470.4-2A.

Some of the methods to detect, assess, deter, and prevent unauthorized access to security areas include the following:
- Barriers must be used to direct the flow of personnel and vehicular traffic through designated entry control points to permit efficient operation of access controls and entry point inspections and to provide the ability to identify and engage adversaries along all feasible pathways.
- Entry control points must be designed to provide a barrier resistant to bypass.
- Permanent barriers must be used to enclose security areas, except during construction or temporary activities, when temporary barriers may be erected.
- Barriers such as fences, walls, and doors may be used to identify the boundary of the PPA and to provide protection. Barriers must be capable of controlling, impeding, or denying access to a security area.
- Fences used should be installed no closer than 20 feet (6 meters) from the building or S&S interest being protected.

d. Describe when random entry/exit inspections are conducted and give reasons for those inspections.

The following is taken from DOE M 470.4-2A.

With the exception of protected and material access areas where inspection is mandatory, random inspections are to be conducted at other designated security area boundaries. The CSA must determine the locations and scope of a screening program at other than PA and material access boundaries. An inspection program must be configured to detect prohibited and controlled articles before being brought into DOE facilities. These programs are to protect Department assets and interests from unauthorized removal without management authorization. Any entry/exit inspection program must be documented in an SSP or procedure.

Random exit inspections are conducted at facility boundaries. The frequency must be determined by DOE line management.

e. List the types of privately owned and controlled articles prohibited from a security area.

The following is taken from DOE M 470.4-2A.

Prohibited articles include the following:

- Explosives
- Dangerous weapons
- Instruments or material likely to produce substantial injury to persons or damage to persons or property
- Controlled substances (e.g., illegal drugs and associated paraphernalia but not prescription medicine)
- Other items prohibited by law

Controlled articles include: portable electronic devices capable of recording or transmitting data (e.g., audio, video, radio frequency, infrared, and/or data link electronic equipment) are not permitted in LAs, EAs, PAs, and MAAs, without prior approval.

22. Safeguards and security personnel with the responsibility for PS must demonstrate a working level knowledge of alarm management and control systems.

a. Discuss the characteristics/capabilities of alarm stations as they relate to monitoring and assessing alarms and initiating response to incidents.

The following is taken from DOE M 470.4-2A.

Alarm stations must provide a capability for monitoring and assessing alarms and initiating responses to S&S events.

- Alarm station personnel must be knowledgeable of the area being protected and the emergency notification procedures.
- Tamper and supervisory alarms must be assessed by authorized personnel and technical/maintenance support personnel according to local procedures.
- Alarm stations must indicate the status of the systems and annunciate a status change. The system must indicate the type and location of the alarm.
- Records must be kept of each alarm received in the alarm station and of any maintenance activities conducted on the alarm system or any of the related components.
- Personnel manning the alarm station must possess an appropriate security clearance (i.e., Q or L) commensurate with the most sensitive interest under the protection of the alarm station.
- Access control systems must ensure admission of authorized personnel only.
- Alarms must annunciate both audibly and visibly to an alarm station.
- Multiple alarms must be prioritized based on the importance of the S&S interests.

Commercial alarms service firms must issue a current UL certification commensurate with the contract service and must maintain this UL certification as long as the service is provided to the facility. For the protection of classified matter UL 2050 should be implemented and a certificate issued for compliance with the UL standard.

b. Discuss the protection and access requirements for facilities holding Category I and II quantities of SNM, or other high-consequence targets as identified by VAs.

Protection

The following is taken from DOE M 470.4-2A.

The priority of protection measures must be designed to prevent malevolent acts such as theft, diversion, and radiological sabotage and to respond to adverse conditions such as emergencies caused by acts of nature. SNM must be protected at the higher level when roll-up to category I quantities can occur within a single security area unless the facility has conducted an analysis that determined roll-up was not credible.

OST is responsible for the promulgation of specific internal guidance governing the protection afforded all DOE matter entrusted to OST for transport by surface and air. Transportation of SNM, whether onsite or by OST, must be provided protection equivalent to that provided by fixed sites for the same material.

- A facility must not possess, receive, process, transport, or store nuclear weapons or SNM until that facility has been cleared.
- An integrated system of positive measures must be developed and implemented to protect category I and II quantities of SNM and nuclear weapons. Protection measures must address physical protection strategies of denial and containment as well as recapture, recovery, and/or pursuit.

- Physical protection for each category of SNM must consider the following factors: quantities; chemical forms; isotopic composition purities: ease of separation, accessibility, concealment, and portability; radioactivity; and self-protecting features.
- The protection of nuclear material production, reactors, and fuel must be commensurate with the category of SNM.
- SNM, parts, explosives, or munitions that are classified must receive the physical protection required by the highest level of classification or category of SNM, whichever is the more stringent.

Category I quantities of SNM must be located within an MAA inside a PA. Any MAA containing unattended category I quantities of SNM must be equipped with an IDS or detection must be provided by PF. Category II quantities of SNM must be located within a PA and under material surveillance procedures. Category III quantities of SNM must be used or processed in an access-controlled security area within at least an LA and in accordance with local security procedures approved by the DOE CSA. Category IV quantities of SNM must be used or processed within at least a PPA and in accordance with local security procedures approved by the DOE CSA.

Category I and II quantities of SNM must be protected by an integrated physical protection system using PF, barriers, and IDAS. IDAS must be designed with independent, redundant data communication lines, intrusion detection and assessment must be immediate, and the video signal must be protected based on the classification level. Video signal would include video signal encryption for conditions wherein video coverage cannot be masked from viewing classified matter. Exterior IDAS are designed to detect unauthorized entry into security areas.

Access

The following is taken from DOE M 470.4-2A.

PAs are security areas typically located within an LA that are established to protect category II or greater quantities of SNM and/or classified matter. The PA provides concentric layers of security for the MAA.

- PAs must be encompassed by physical barriers that identify the boundaries, surrounded by PIDAS, and equipped with access controls that ensure only authorized personnel are allowed to enter and exit.
- An inspection program must ensure prohibited and controlled articles are detected before being brought into PA facilities.
- When the PIN or biometric system is either not working or not implemented at security areas requiring measures in addition to access control, PF or other trained security personnel must perform the access control requirements as documented in the SSP.

Personnel access control:

- Unescorted access must be controlled to limit entry to individuals with L or Q security clearance.

- Visitor logs must be used for PAs.
- Validation of the security clearance must occur at PA entry control points.

Vehicle access controls:

- Private vehicles are prohibited.
- Government-owned or -leased vehicles or delivery vehicles may be admitted only when on official business and only when operated by properly cleared and authorized drivers or when drivers are escorted by properly cleared, authorized personnel.
- Vendor vehicles are prohibited unless the vehicles and drivers have been subjected to a thorough inspection/investigation and been given access approval by the DOE CSA.
- Entrance inspections of all personnel, vehicles, packages, and hand-carried items must be performed to deter and detect prohibited and controlled articles.

MAAs are security areas that are established to protect category I quantities of SNM. In addition to requirements for a PA the following apply to an MAA:

- Access control must be administered by armed PF personnel and/or automated access control systems.
- Entry is limited to personnel with a Q security clearance and who have been authorized for entry consistent with need-to-know and operations.
- Individuals without appropriate security clearance must be escorted.
- S&S interests, not in approved storage within an MAA, must be controlled by the custodian or authorized user.
- Validation of security clearance must occur at MAA entry control points.
- Site-specific requirements and procedures for visitors must be developed and approved by DOE line management.
- Security requirements for entry/exit inspection must be established by DOE line management and documented in the SSP.

23. Safeguards and security personnel with the responsibility for PS must demonstrate a working level knowledge of protection of security system elements.

a. Describe how security-related equipment must be protected from unauthorized access in a graded manner consistent with the security interest under protection.

The following is taken from DOE M 5632.1C-1 (archived).

Strategies for the physical protection of SNM and vital equipment shall incorporate the applicable requirements established in DOE M 5632.1C-1 (archived), chapter II. Protection strategy may be graduated to address varying circumstances and may range from denial to containment.

By graded approach, DOE intends that, in the development and implementation of protection and control programs, the level of effort and magnitude of resources expended for the protection of a particular security interest are commensurate with the security interest's

importance or the impact of its loss, destruction, or misuse. Interests whose loss, theft, compromise, and/or unauthorized use will have serious impact on the national security, and/or the health and safety of DOE and contractor employees, the public, the environment, or DOE programs, shall be given the highest level of protection. For example, use of a WMD by a terrorist(s) could have consequences so grave as to demand the highest reasonably attainable standard of security. Protection of other interests shall be graded accordingly. Asset valuation, threat analysis, and VAs shall be considered, along with the acceptable level of risk and any uncertainties, to decide how great the risk and what protection measures are to be applied. Heads of departmental elements shall provide a rational, cost-effective, and enduring protection framework using risk management as the underlying basis for making security-related decisions. It should be recognized that risks will be accepted; (i.e., that actions cannot be taken to reduce the potential for or consequences of all malevolent events to zero); however, an acceptable level of risk will be determined based on evaluation of a variety of facility-specific goals and considerations. Protection-related plans shall describe, justify, and document the graded protection provided the various S&S interests.

24. Safeguards and security personnel with the responsibility for PS must demonstrate the ability to review and access the contractor's protection program.

a. Conduct an assessment of the contents and accuracy of the contractor's protection and control planning.

b. Assess the contractor's methods for protecting SNM and vital equipment.

c. Assess the contractor's program for protecting and controlling classified matter and computer resource assets.

d. Assess the contractor's program for establishing, controlling, and maintaining security and restricted access areas.

e. Assess and approve the protection elements established by the contractor.

These are performance-based KSAs. The Qualifying Official will evaluate their completion.

C. PROTECTIVE FORCE OPERATIONS (PFO)

Competencies and supporting knowledge and skills for section C, Protective Force Operations, are derived from the following DOE Orders, manuals, and guides:

- 10 CFR 1047, "Limited Arrest Authority and Use of Force by Protective Force Officers"
- DOE O 440.1B, *Worker Protection Program for DOE (including the National Nuclear Security Administration) Federal Employees*
- DOE O 440.2B chg 1, *Aviation Management and Safety*
- DOE O 470.4A, *Safeguards and Security Program*
- DOE O 470.3B, *Graded Security Protection (GSP) Policy*

- DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*
- DOE M 470.4-1 chg 1, *Safeguards and Security Program Planning and Management*
- DOE M 470.4-2 chg 1, *Physical Protection*
- DOE M 470.4-3 chg 1, *Protective Force*
- DOE M 470.4-3A, *Contractor Protective Force*
- DOE M 470.4-6 chg 1, *Nuclear Material Control and Accountability*
- DOE M 471.1-1 chg 1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*
  [Note: DOE M 470.4-2 chg 1 has been superseded by DOE M 470.4-2A; DOE M 470.4-3 chg 1 has been superseded by DOE M 470.4-8, *Federal Protective Force*.]

25. Safeguards and security personnel with the responsibility for PFO must demonstrate a working level knowledge of the planning for PFO.

a. Discuss the planning requirements to ensure appropriate response or defense by the site PFs.

The following is taken from DOE M 470.4-8.

In accordance with integrated S&S management practices, and in support of the DOE S&S protection program management requirements, Federal protective force (FPF) programs, functions, or activities must incorporate basic planning principles to ensure that they accomplish their intended purpose.

- FPF programs/elements, regardless of size, must clearly identify the mission to be fulfilled by the organization. Broad mission statements may be supported by establishing more specific goals and objectives for the FPF element to achieve.
- FPF programs/elements must document resources requirements necessary to successfully accomplish mission objectives. Resource requirements may be identified as, but not limited to, the following:
  - The number of projected Federal agent (FA) man-hours to support scheduled movements of material between sites
  - The number of Federal officer man-hours to support scheduled activities
  - The number of projected special agent (SA) man-hours to support scheduled executive protection details
  - Equipment items necessary to support such operations
- Authorizations may be identified in terms of full-time equivalents, the total number of personnel needed, total number of direct man-hours, and/or quantities of equipment items needed to perform work. Authorizations necessary to fulfill resource requirements are determined by factoring in various considerations such as, but not limited to the following:
  - Established shift schedules
  - Training requirements
  - Relief factors

- Travel distances
- Operational effectiveness
- Unit readiness
- Performance testing
- Equipment maintenance

- FPF programs/elements must maintain a process that monitors and periodically reports actual personnel and sensitive equipment items currently on hand. Actuals differ from authorizations in that actual numbers of personnel on hand will generally fall short of authorizations; however, on occasion situations may require that actual exceed authorizations. Approval to temporarily exceed personnel authorizations must be obtained from DOE line management.

The following is taken from DOE M 470.4-3A.

Contractor PF missions/functions match Federal PF missions/functions except for the following:

- Required plans include:
  - Security incident response plan (SIRPs) covering response requirements to security incidents; adversary intrusion of a facility/site; and defense against adversary use of weapons, explosives, and chemical/biological weapons (CBW) is described in DOE O 470.3B.
  - Security contingency response plans covering PF work stoppages, PF recall measures, and response actions of local, state, and Federal law enforcement agencies (LEAs) as documented by vulnerability analysis.
- Target folders must be developed and maintained by TRF sites and/or those with radiological sabotage concerns. Target folders should be sufficient to provide information necessary to assist the PF and outside agencies in conducting interagency compatible tactical operations.

b. Describe the purpose of the following types of plans as they relate to PFO:

- **Security Incident Response Plans**
- **Facility Evacuation Response Plans**
- **Security Contingency Response Plans**
- **Target folders**
- **Fresh pursuit for property or SNM theft**

Security Incident Response Plans

The following is taken from DOE M 470.4-3A.

SIRPs cover response requirements to security incidents; adversary intrusion of a facility/site; and defense against adversary use of weapons, explosives, and CBW as described in the current DOE O 470.3B. SIRPs must provide specific response directions and required actions to PF personnel for applicable containment, denial, recapture, recovery, and pursuit strategies and to support interruption/neutralization operations before completion of

adversary task time. When a site facility VA, performance test (PT), and/or SSP dictate a recapture strategy, PF personnel must have the ability to gain entry to the target facility in accordance with SSP/VA timeliness.

Facility Evacuation Response Plan

The following is taken from DOE M 473.2-2 chg 1 (archived)

Facility evacuation response plans cover protection of security interests, employees, the public, and the environment during nuclear release incidents, adversary use of CBW, radiological/toxicological/industrial sabotage, and other site emergencies.

Security Contingency Response Plans

The following is taken from DOE M 470.4-3A.

Security contingency response plans cover PF work stoppages, PF recall measures, and response actions of local, state, and Federal LEAs as documented by vulnerability analysis. See DOE G 473.2-1, *Guide for the Establishment of a Contingency Protective Force*, (archived), for more details.

Target Folders

The following is taken from DOE M 470.4-3A.

Target folders must be developed and maintained by TRF sites and/or those with radiological sabotage concerns. Target folders should be sufficient to provide information necessary to assist the PF and outside agencies in conducting interagency compatible tactical operations.

The following is taken from DOE M 471.2-2 chg 1 (archived).

Target folders, containing interagency compatible site descriptions and response planning documentation along with facility-specific information (e.g., engineering descriptions of buildings, entry/exit locations, response and observation positions, types and quantities of SNM or other attractive targets and their locations, critical paths, etc.) to assist the PF and outside LEA in conducting interagency compatible tactical operations.

Fresh Pursuit for Property or SNM Theft

The following it taken from DOE M 470.4-8.

Fresh pursuit is (with or without a warrant) for the purpose of preventing the escape or effecting the arrest of any person who has committed a misdemeanor or felony or is suspected of having committed a misdemeanor or felony. Fresh pursuit implies pursuit without unreasonable delay but need not be immediate pursuit. [Although fresh pursuit implies pursuit without unreasonable delay, to prevent the escape or to arrest fleeing suspected criminals who are in unauthorized control or possession of nuclear weapons, weapons components, and/or SNM, such pursuit must be effected immediately.]

c. Describe the principle and applicability of non-Departmental law enforcement agency support.

The following is taken from DOE M 470.4-8.

When other Federal, state, or local LEAs with jurisdiction in the area into which the suspected criminal has fled join the pursuit, they must be primarily responsible for the continued pursuit except when the suspected criminal is in possession of DOE nuclear security assets.

- The FPF dispatcher, supervisors in the FPF command structure, and the officer in charge of FPF operations must coordinate the pursuit efforts of FPF officers with other Federal, state, and/or other local LEAs.
- FPF officers participating in the pursuit must continue to participate in pursuit operations until otherwise instructed by the FPF dispatcher, respective supervisors in the FPF command structure, or the officer in charge of FPF operations.
- At least one FPF officer unit will remain available to assist the other pursuing Federal or state and other local LEA until the pursuit is concluded or otherwise terminated. That FPF officer will thereafter provide such LEA with all relevant information regarding the circumstances surrounding the incident.

d. Describe the levels, associated responsibilities, and qualification requirements of PF personnel within DOE.

The answer to this question depends upon PF personnel performing as contractors or Federal employees.

The following is taken from DOE M 470.4-3A.

The levels of PF contractor personnel are as follows:

- SOs must meet the training, qualification, and medical requirements in 10 CFR 1046, subpart B.
- SPOs must meet the medical, physical fitness, firearms, and training and qualification requirements in 10 CFR 1046, subpart B.
- SPOs are broken down into SPO-I, SPO-II, and SPO-III, depending on level of skill and training.

The formal training and qualification program must be based on a valid and complete set of job tasks, with identified skills and knowledge needed. KSAs necessary to competently perform the tasks associated with assigned PF duties must be identified based upon the applicable job analysis (JA) applicable for each job assignment. PF personnel must demonstrate familiarity with, and knowledge of, the responsibilities identified in the JA for their assignment and must demonstrate proficiency in the skills and abilities necessary to perform required and assigned job tasks. All PF personnel must demonstrate the following:

- Knowledge of, and ability to perform safely, routine and emergency duty requirements

- Operation of assigned equipment and vehicles
- Operation of communication equipment
- Knowledge of, and the ability to apply, DOE directives, policies, plans, standard operating procedures, specific operational instructions, Orders and procedures governing assigned routine and emergency duties
- Knowledge of Federal- and state-granted authority applicable to assigned activities and responsibilities between PF and other LEA
- Knowledge of security practices and procedures

Qualification requirements—PF personnel must comply with the departmental medical, physical fitness, and firearms qualifications and training requirements as appropriate in 10 CFR 1046.

Security clearance—PF personnel must possess a security clearance commensurate with the highest level of classified information or matter to which they have, or potentially have, access. SPOs must possess L or Q security clearances. SPOs with access to nuclear weapons, nuclear test devices, or complete nuclear assemblies; category I and II quantities of SNM; fully automatic weapons; or who are assigned to offensive posts must possess Q security clearances. All PF personnel with security clearances are subject to the Department's random drug-testing requirements.

Medical, physical fitness—SOs and SPOs must meet the medical, physical fitness, firearms, and training and qualification requirements in 10 CFR 1046; subpart B.

Special skills qualifications—site-specific conditions may justify requirements for PF personnel to possess qualifications for special skills (e.g., security helicopter operations, ascending and descending techniques, mechanical and explosive tactical entry techniques, CBW countermeasures, hostage negotiation, precision rifleman/forward observer team, communications, exercise controllers/evaluators, remotely operated weapons systems, or alarm station monitoring). Certifications required for specific job functions must be kept current.

Firearms—no person will be authorized to carry a firearm as a PF officer until the individual is qualified according to the approved firearms qualification standards. Each SPO must qualify with each firearm that is reasonably expected to be used during duty assignment on the qualification course indicated in the DOE-approved firearms qualification courses and any applicable approved site-specific supplemented qualification course. The employing organization must maintain written documentation indicating each individual who is authorized to carry firearms and make arrests without warrant while performing official duties.

The following is taken from DOE M 470.4-8.

The levels of Federal PF personnel are: Federal officers (FOs), FAs, and SAs.

The responsibilities of FOs may or may not possess firearms/arrest authority pursuant to section 161k of the Atomic Energy Act or section 661 of the DOE Organization Act, and must, when directed

- conduct investigations
- conduct liaison activities with law enforcement officials
- perform inquiries into local and national security issues
- conduct interviews
- conduct surveys and inspections

Qualification requirements: FOs must possess security clearances commensurate with the highest level of classified information or matter to which they have, or potentially have, access. Armed FOs must complete a formal training and qualification program before being assigned to duties. The training program must be based on assigned functions. Firearms, physical fitness, and medical qualifications must meet DOE requirements for the position assignment as described in DOE M 470.4-8, chapter I.

FAs are career professionals who are specially trained for a unique job. They devote themselves to career and subsequently retire. FA duty positions require individuals to be physically tough, mentally fit, and highly trained to perform assigned duties and qualification requirements commensurate with their duty positions. FA trainees are newly appointed FAs serving in the position for less than one year and in a one-year probationary period, in a specific OJT program. Upon completion of the OJT program the FA trainee is promoted to an FA.

FA positions are FAs serving in an assigned duty position for one year or more and who meet the subject standards and requirements. These positions include: FA, Nuclear Materials Courier (NMC); Senior FA NMC (vehicle commander); Lead FA NMC (convoy commander); and Supervisory FA (squad leader).

Qualification requirements: FAs receive initial training and qualification in the agent candidate training program, which encompasses the following subject matter categories: driving, firearms, intermediate use of force, and tactics.

Armed DOE Federal employees designated as SAs by the Chief Health, Safety and Security Officer possessing firearms/arrest authority pursuant to section 161k of the Atomic Energy Act, may be deputized by the U.S. Marshals Service, and must, when directed

- participate in special operations such as executive protection
- conduct investigations
- conduct liaison activities with law enforcement officials
- perform inquiries into local and national security issues

The training and qualification programs used by the Special Operations Program will be based on criteria established by the Federal Law Enforcement Training Center (FLETC) or will have Federal Law Enforcement Training Accreditation. The Special Operations Program training program will be based on the SA Professional Qualification Program (PQP). The

PQP is part of a career-long learning continuum for SAs that will include advanced education, formal training, individual qualifications, individual learning opportunities, and experienced-based learning. SAs will qualify with all duty weapons according to DOE M 470.4-8, chapter V by successfully completing the appropriate DOE or FLETC firearms qualification courses under both daylight and reduced lighting conditions.

e. Discuss the authority and responsibility for issuing credentials and shields for each level of PF personnel within DOE.

The following is taken from DOE M 470.4-3A.

Credentials and shields are issued to qualified DOE contractor personnel to identify the bearer as having the authority to perform assigned official duties. The design of all S&S credentials and shields used by contractor PFs must be approved by the Chief Health, Safety and Security Officer, and where applicable DOE line management.

Fulfillment of training and qualification requirements for the position or duties must be verified before issuing a credential or credential with shield to an individual. The issuing authorities for contractor security credential and the SPO with shield (armed) are the Director, Office of Headquarters Security Operations and the DOE CSA for their respective organizations.

The following is taken from DOE M 470.4-8.

Credentials and shields are issued to qualified DOE Federal employees and FOs/FAs/SAs to identify the bearer as having the authority to perform assigned official duties only. The design of all S&S credentials and shields must be approved by the DOE Chief Health, Safety and Security Officer and, where applicable, DOE line management.

Fulfillment of training and qualification requirements for the position or duties must be verified before issuing a credential or credential with shield to an individual. The issuing authorities for the FO credential with shield (unarmed), the FO credential with shield (armed), and the SA are the Director, Office of Security Operations or the DOE CSA for their respective organizations. The issuing authority for NNSA FO credentials and shields is the Associate Administrator for Defense Nuclear Security. The issuing authority for OST credential with shield (armed) is the Assistant Deputy Administrator for Secure Transportation.

f. Discuss the general guidelines for fresh pursuit.

The following is taken from DOE M 470.4-8.

The purpose of these guidelines is to set forth the procedures to be followed by DOE PF personnel when pursuing suspected criminals across jurisdictional lines, except when the suspected criminals are in possession of DOE security assets.

It is DOE policy to prevent the escape and to effect the arrest of fleeing suspected criminals in a safe and expeditious manner. The following procedures are intended to provide protective personnel with flexibility when in fresh pursuit of a fleeing suspected criminal. Each site/organization must prepare guidelines that take into account the geography, equipment, and functions of the facility/site and that address the procedures that will be used to provide emergency notification to jurisdictions that may be entered in a fresh pursuit situation. The DOE CSA must submit the guidelines through the cognizant departmental element to the Chief Health, Safety and Security Officer, for approval. The approval authority for NNSA site/organizations is the Associate Administrator for Defense Nuclear Security.

The following is taken from DOE M 470.4-3A and DOE M 470.4-8.

Fresh pursuit procedures:

- Responsibility for decisions respecting fresh pursuit must follow the FPF command structure. In making fresh pursuit decisions, FPF officers must consider applicable Federal and state laws; Department directives, guidelines, and regulations; and FPF plans, Orders, guidelines, and training.
- Safety is a primary consideration when engaged in fresh pursuit of a suspected criminal. In determining whether to pursue, as well as the method and means of pursuit, an FPF officer will weigh the seriousness of the alleged offense and the necessity for immediate apprehension against the risk of injury to himself/herself, other FPF officers, and the public. If, at any time during the pursuit, the risk of injury to pursuing FPF officers or the public surpasses the necessity for immediate apprehension, the pursuit must be terminated.
- FPF officers will use the minimum force necessary under the circumstances to apprehend a suspected criminal.
- Regulations at 10 CFR 1047.6, "Use of Physical Force When Making An Arrest," 1047.7, "Use of Deadly Force," 1049.6, "Exercise of Arrest Authority—Use of Non-Deadly Force," and 1049.7, "Exercise of Arrest Authority—Use of Deadly Force," address the applicability of physical and/or deadly force in a fresh pursuit situation, regardless of whether jurisdictional lines have been crossed. Such use may include, as appropriate, firing at or from a moving vehicle, aircraft, or water craft; the ramming and disabling of pursued vehicles by precision immobilization techniques (PIT); and the use of tire-deflating devices.
- If hostages are present in a pursuit situation in which recovery of SNM is involved, the safety and welfare of hostages must be considered; however, due to the ramifications of unauthorized use of SNM to the national security, the public, and the environment, the hostages' presence must not deter or impact immediate pursuit and recovery of the SNM.
- Vehicular pursuit:
    - Vehicles used in fresh pursuit must be operated in as safe a manner as is practicable.

- To the extent practicable, vehicles used must be marked and equipped with visual and audible emergency equipment.
- Vehicles occupied by non-FPF personnel must not be used in fresh pursuit situations unless the situation mandates an immediate pursuit and the extreme circumstances prohibit the occupant's disembarkation.
- The number of pursuing vehicles that cross a jurisdictional line must be limited to that necessary to provide sufficient personnel to deal with the situation. Under no circumstances will the number of pursuing FPF officers be such that the assets are left without sufficient security protection.
- There are inherent dangers associated with the use of roadblocks; thus, unless exigent circumstances mandate immediate apprehension of the suspected criminal (e.g., unauthorized control of SNM, possession of explosives), FPF officers generally must not attempt roadblocks without the authorization of the appropriate law enforcement officials of the jurisdiction entered and must not use roadblocks to apprehend suspected misdemeanants without the concurrence of the supervisor of the pursuing FPF officers.
- There are inherent dangers associated with the use of ramming/PIT and tire deflating devices; thus, unless exigent circumstances mandate immediate disabling of the suspect vehicle, FPF officers generally must not attempt ramming/PIT or use tire deflation devices without the authorization of an FPF supervisor.

- Where DOE has aerial capability (helicopters or fixed-wing aircraft), specific guidelines regarding the use of aircraft in fresh pursuit situations including pursuit, observation, reporting, and deployment of response forces must be coordinated with appropriate state and other local officials.
- Where DOE has waterborne capability, specific guidelines regarding the use of water craft in fresh pursuit situations including pursuit, observation, reporting, and deployment of response forces must be coordinated with appropriate state and other local officials.
- At all times during a fresh pursuit situation, the FPF officers involved must make every attempt practicable to maintain open communications and to relay as much information as possible to the FPF dispatcher and/or FPF chain of command.

26. Safeguards and security personnel with the responsibility for PFO must demonstrate a working level knowledge of PF duties.

a. Discuss the general duties and response categorization requirements of the three PF levels.

The following is taken from DOE M 470.4-3A.

Response Categorization

Medical and physical fitness requirements for each PF position are based on the expected level of physical exertion associated with security response duties. Duty assignments for each PF position, including supervision, must be clearly identified to ensure that assigned personnel are qualified to perform required duties. Response deployment must be consistent with facility-specific VAs as documented in the site's approved SSP. Three response categories have been established based on the duties outlined below. The following categorizations apply to PF facilities:

- Active defense (offensive combatant—SPO-II & -III)
- Static defense (defensive combatant—SPO-I)
- Response support (non-combatant—SO)

Security Police Officers I

Duty assignments:

- TRF facilities—fixed fighting positions, armored vehicles with an expectation of employing the capabilities of the vehicle, towers, access control, alarm monitoring, dispatch, security checks, armed construction/administrative escort, and material/package inspection.
- Non-TRF facilities—fixed fighting positions, armored vehicles with an expectation of employing the capabilities of the vehicle, and foot patrols, alarm response and assessment, access control, alarm monitoring, dispatch, security checks, armed construction/administrative escort, and material/package inspections.

Security Police Officers II

Duty assignments: vehicle and foot patrols, mobile and mobile reserve response force with the primary mission of denying adversary access to targets.

Security Police Officers III

Duty assignments: TFR facilities. Exterior reconnaissance patrols, SRT posts, activities and duties with the primary missions of recapture, recovery, and pursuit.

Security Officers

Duty assignments: where practicable, unarmed SOs should be used to perform administrative, access control, facility patrol, escort, alarm assessment, alarm monitoring, and dispatch duties and to report alarms. SOs will enforce S&S protection requirements to allow, as appropriate, armed PF personnel to maintain focus on their primary mission of combating the armed terrorist threat.

b. Discuss how responsibilities identified in a PF job analysis relate to proficiency in the skills and abilities necessary to perform job tasks.

The following is taken from DOE M 470.4-8.

The training program must be based on a valid and complete set of job tasks with identified levels of skills and knowledge needed. KSAs necessary to competently perform the tasks associated with assigned FO duties must be identified based on the JA applicable for each job assignment. FOs must demonstrate familiarity with, and knowledge of, the responsibilities identified in the JA for their assignment and must demonstrate proficiency in the skills and abilities necessary to perform required assigned job tasks.

c. Discuss the use of deadly force and limited arrest authority as set forth in 10 CFR 1047, Limited Arrest Authority and Use of Force by Protective Force Officers.

The following is taken from 10 CFR 1047.7.

Deadly Force

A PF officer is authorized to use deadly force only when one or more of the following circumstances exist:

- Self defense—when deadly force reasonably appears to be necessary to protect a PF officer who reasonably believes himself or herself to be in imminent danger of death or serious bodily harm.
- Serious offences against persons—when deadly force reasonably appears to be necessary to prevent the commission of a serious offense against a person(s) in circumstances presenting an imminent danger of death or serious bodily harm.
- Nuclear weapons or nuclear explosive devices—when deadly force reasonably appears to be necessary to prevent the theft, sabotage, or unauthorized control of nuclear weapon or nuclear explosive devices.
- Special nuclear material—when deadly force reasonably appears to be necessary to prevent the theft, sabotage, or unauthorized control of SNM from an area of a fixed site or from a shipment where category II or greater quantities are known or reasonably believed to be present.
- Apprehension—when deadly force reasonably appears to be necessary to apprehend or prevent the escape of a person reasonably believed to: have committed an offense of the nature specified in 10 CFR 1047.7, paragraphs (a)(1) through (a)(4); or be escaping by use of a weapon or explosive or who otherwise indicates that he or she poses a significant threat of death or serious bodily harm to the PF officer or others unless apprehended without delay.
- Additional considerations involving firearms—if it becomes necessary to use a firearm, the following precautions shall be observed:
  - A warning (e.g., an order to halt) shall be given, if feasible, before a shot is fired; and
  - Warning shots shall not be fired.

Limited Arrest Authority

The following is taken from 10 CFR 1047.4.

Under the Atomic Energy Act (AEA), the authority of a DOE PF officer to arrest without warrant is limited to the performance of official duties and should be exercised only in the enforcement of the following laws:

- Only if property of the U.S. which is in the custody of the DOE or its contractors is involved:
  - Arson
  - Building or property within special maritime and territorial jurisdiction
  - Civil disorder
  - Communication lines, stations, or systems
  - Concealment, removal, or mutilation generally
  - Conspiracy
  - Destruction of motor vehicles or motor vehicle facilities
  - Explosives
  - Government property or contracts
  - Military, naval, or official passes (pertains to forging or altering official passes)
  - Personal property of the U.S.
  - Public money, property, or records
  - Sabotage
  - Violation under the Physical Security Convention
- A PF officer is authorized to make an arrest for any felony listed in 10 CFR 1047.4, "Arrest Authority," if the offense is committed in the presence of the PF officer or if he or she has reasonable grounds to believe that the individual to be arrested has committed or is committing the felony.
- A PF officer is authorized to make an arrest for any misdemeanor listed in 10 CFR 1047.4, if the offense is committed in the presence of the PF officer.
- The AEA does not provide authority to arrest for violations of state criminal statutes or for violations of Federal criminal statutes other than those listed in 10 CFR 1047.4.
- Those locations which are within the "special maritime and territorial jurisdiction of the U.S.," as defined in 18 U.S.C. 13, "Laws of States Adopted for Areas Within Federal Jurisdiction," adopt the law of the state for any crime under state law not specifically prohibited by Federal statute and provide for Federal enforcement of that state law.

d. Describe DOE's policy for rules of engagement for the use of PF and remotely-operated weapons systems.

The following is taken from DOE M 470.4-8.

DOE's use of deadly force policy, as set forth in 10 CFR Part 1047 defines the circumstances when deadly force is authorized, (i.e., self-defense; serious offenses against persons; theft, sabotage, or unauthorized control of nuclear weapons, nuclear explosive devices, or SNM); and apprehension. It also states, "Its use may be justified only under conditions of extreme necessity, when all lesser means have failed or cannot reasonably be employed." DOE has determined that the CFRs concept of, "or cannot reasonably be employed," needs further

site-specific amplification in the post September 11, 2001 environment. To ensure acceptable protection of critical assets, site-specific rules of engagement (ROE) are needed that define the circumstances, (e.g., location, time, and distance at each site) when lesser means of force cannot reasonably be employed. ROE must address the concept of hostile intent as described in DOE M 470.4-3A and DOE M 470.4-8.

Each DOE site with forces having the mission of protecting nuclear weapons, SNM, and/or other hazardous material that may be used as a weapon of mass destruction must develop site-specific ROE that incorporate the concept of hostile intent.

The determination of site-specific ROE must consider the type of materials being protected, site geography, building construction, PF strength and capability, adversarial task times, adversarial characteristics as described in the current DOE O 470.3B and consequences of asset loss. ROE must clearly state under what conditions the circumstances of hostile intent have been met. Depending on site-specific conditions, the circumstance of hostile intent may be met even if no shots have been fired.

This paragraph is taken from DOE M 470.4-8 and DOE M 470.4-3A.

The potential use of new weapon systems, (e.g., directed energy and remotely-operated weapons systems), within DOE is consistent with 10 CFR Part 1047 and should be considered when formulating ROE. It is DOE policy that a human being must make a conscious decision to employ all weapons systems capable of delivering deadly force before each operation of such equipment, (i.e., fully automated use is not permitted).

e. Describe the following safety, training, authorization requirements for an armed PF:
- **Firearms safety procedures related to duty weapons**
- **Firearms training and qualification requirements for all duty weapons**
- **Application of the authorization to carry firearms and make arrests without a warrant while performing official duties**

The following is taken from DOE M 470.4-3A.

Firearms Safety Procedures Related to Duty Weapons

The four general firearms safety rules are:
- All firearms are always loaded.
- Never point a firearm at anything you are not willing to destroy.
- Keep your finger off the trigger until your sights are on the target.
- Be sure of your target.

Firearms Training and Qualification Requirements for all Duty Weapons

Basic training:
- Basic firearms safety training, demonstrated technical knowledge, and practical proficiency is required before firearms are permitted to be carried on duty. Safety

training must be conducted semiannually (at least every 6 months), at which time safety proficiency must be demonstrated in order to retain weapon-carrying status.

- Basic firearms training must be conducted at a site approved by the DOE CSA.
- Basic firearms safety training must include the following:
  - General firearms safety orientation
  - Instructions on the capabilities of firearms and ammunition and their implications and instructions on hazards associated with the impact of bullets and other projectiles on nuclear explosives, nuclear weapons, explosives, and other possible items known to be on site that could result in a significant release of energy or toxic substances
  - Firearms safety information for each type of firearm required by duty assignment
  - Practice with the unloaded firearm in the teaching environment
  - Range safety procedures and demonstration of safe firing techniques on the range
  - Dry-firing techniques and hazards associated with dry firing
  - Handling of misfires
  - Detailed procedures on clearing, handling of malfunctions, inspecting, cleaning, loading, unloading, and other specific tasks related to each firearm for which the student receives training
  - Details of firearms accidents and how they could have been prevented
  - The four general firearms safety rules
- Advanced firearms training will following the above requirements.
- Application of the authorization to carry firearms and make arrests without a warrant while performing official duties.

Authority to Carry Firearms:

- The employing organization must maintain written documentation indicating each individual who is authorized to carry firearms and make arrests without warrant while performing official duties.
- Firearms instructors who are not currently assigned SPO duties may carry firearms when performing their instructional duties if authorized by DOE line management. These instructors must pass the firearms qualification courses for assigned firearms and for firearms that are the subject of instruction.

A PF officer is authorized to make an arrest for any felony covered under their limited arrest authority if the covered offense is committed in the presence of the PF officer or if the PF officer has reasonable grounds to believe (e.g., information from another PF or law enforcement officer, communications from a PF dispatcher, or CAS operator) that a suspect had committed or was committing a felony.

For more information on this subject consult 10 CFR 1047.4.

27. Safeguards and security personnel with the responsibility for PFO must demonstrate a working level knowledge of the Special Response Team (SRT).

a. Discuss mission requirements of a SRT as they relate to the following:

- **Interdiction**
- **Interruption**
- **Neutralization**
- **Containment**
- **Denial**
- **Recapture**
- **Recovery**
- **Pursuit**

The following is taken from DOE M 470.4-3A.

The mission of the SRT is to resolve incidents that require force options that exceed the capability of SPO-I and –II personnel and/or existing PS systems. The SRT must be capable of effective and ready response. The SRT must be trained and equipped to conduct interdiction, interruption, neutralization operations, and containment, denial, recapture, recovery, and pursuit strategies directed against an adversary.

- An SRT is required at TRF facilities and for intra-site transport of denial targets.
- A contractor request for authorization to deploy an SRT capability at a site or facility that does not meet requirements in DOE M 470.4-3A, chapter VIII, paragraph 1a, must be approved by DOE line management with notification to the cognizant departmental element. Approvals must be based on a site VA that documents the need for an SRT (e.g., a radiological/toxicological/sabotage target that could have adverse impact on national security, the health and safety of employees, the public, or the environment).
- The SRT must be staffed with qualified and certified SPO-III personnel deployed as one or more dedicated teams with specialized weapons and equipment, operating from mobile tactical vehicles, as ground assault forces, or a combination of both.

An SRT must be capable of resolving adversary actions using force options (including, but not limited to, open-air, mobile, stronghold, and emergency assault using dynamic and covert techniques) and team tactics for interdiction, interruption, neutralization, containment, denial, recapture, recovery, and pursuit operations.

b. Discuss the mission and special training requirements of Precision Rifle Forward Observer Team members and Tactical Entry Specialists.

The following is taken from DOE M 470.4-3A.

The mission of PF positions include both armed and unarmed positions for the purpose of protecting DOE assets including facilities, personnel, sensitive materials, and other property against threats identified in DOE O 470.3B.

Special training—team members may volunteer and/or be selected for specialized SPO-III duties for which the following requirement must be met.

Precision Rifleman Forward Observer Team (PRFOT)—before initial assignment to duty as a PRFOT member, each assigned SPO-III must successfully complete the DOE PRFOT training course approved by the Office of Health, Safety and Security. Thereafter, on a quarterly basis, each PRFOT member must participate in live- and dry-fire proficiency training. Live- and dry-fire proficiency training must be integrated into and conducted in conjunction with SRT training via controlled use of force, tactical movement training, and night operations.

Tactical Entry Specialist training—before initial assignment to Tactical Entry (TE) specialist duties, each SPO-III assigned must successfully complete the DOE basic TE course approved by the Office of Health, Safety and Security. Thereafter, each specialist must participate quarterly in proficiency training that includes mechanical entry techniques. Before conducting explosive TE operations, specialists must successfully complete an explosive TE course approved by the Office of Health, Safety and Security.

c. Discuss the SRT program certification/recertification requirements.

The following is taken from DOE M 470.4-3A.

SRT programs must be certified initially and recertified annually (at least every 12 months) by the DOE CSA. A program is considered certified/recertified when the site has completed the following validations:

- All assigned SRT members have met the training requirements of DOE M 470.4-3A.
- The DOE CSA has determined that the site SRT program is in compliance with this contract requirements document (CRD) and has forwarded documentation of the satisfactory completion of site certification/recertification to the cognizant departmental element.
- All of the above can be accomplished during the annual periodic S&S survey.

28. Safeguards and security personnel with the responsibility for PFO must demonstrate a working level knowledge of PF training and qualification.

a. Discuss the requirement for developing and revising a job analysis for PF positions.

The following is taken from DOE M 470.4-3A.

JAs (e.g., a list of common tasks required for PF assignments) must be prepared and reviewed annually (at least every 12 months) for positions directly related to protective operations. JAs must be used as basic input documents to local training requirements. JAs must address site-specific requirements for activities that have not been standardized and issued by the DOE NTC.

b. Discuss the required elements of a PF training program.

The following is taken from DOE M 470.4-3A.

The formal training and qualification program must incorporate the following:

- Be based on a valid and complete set of job tasks, with identified levels of skills and knowledge needed. KSAs necessary to competently perform the tasks associated with assigned PF duties must be identified based upon the JA applicable for each job assignment. PF personnel must demonstrate familiarity with, and knowledge of, the responsibilities identified in the JA for their assignment and must demonstrate proficiency in the skills and abilities necessary to perform required and assigned job tasks. All PF personnel must demonstrate
  - knowledge of, and ability to perform safely, routine and emergency duty requirements;
  - operation of assigned equipment and vehicles;
  - operation of communication equipment employed, including proficiency in accepted communication terminology, acronyms, and phonetics, and the methods for verifying operator identity of incoming signals and signaling duress;
  - knowledge of, and the ability to apply, DOE directives, organization policies, plans, standard operating procedures, specific operational instructions, Orders, and procedures governing assigned routine and emergency duties;
  - knowledge of Federal- and state-granted authority applicable to assigned activities and responsibilities between the PF and other law enforcement authorities; and
  - knowledge of security practices and procedures, including the following, as applicable:

    - access control procedures and operations including DOE security clearance and security badging requirements;
    - DOE security area designations and related prohibited article restrictions;
    - inspection techniques they may be responsible for using on persons, packages, and vehicles;
    - operation of inspection equipment, (e.g., X-ray, magnetometers, radiation detectors);
    - procedures for escorting personnel within security areas;
    - implementation of plans, Orders, and procedures to protect DOE interests during disruptive events;
    - recognition of, and storage locations for, S&S interests they are responsible for protecting;
    - responsibility and processes to report incidents, violations, and anomalous conditions;
    - awareness of the types of, and threats posed by, WMD and improvised explosive devices borne by vehicles/personnel; and
    - use of assigned personal protective equipment.

- Aim at achieving a well-defined level of competency; specifically, mission accomplishment and survival.
- Employ standardized lesson plans with clear performance objectives as a basis for instruction. Lesson plans in regular use must be reviewed for currency any time training requirements are changed and must be reviewed and/or revised for currency before training is conducted.
- Include frequent, performance-based, and realistic simulation testing to determine individual and small unit tactical skills and leadership and to certify job readiness.
- Be documented so individual and overall training status is easily accessible (individual training records must be retained until one year after an employee is terminated as a PF member unless other requirements specify a longer retention period).
- Consider the learning characteristics and entry-level competencies of trainees.

c. Discuss the special training requirements required to support the maintenance of a qualified instructor cadre.

The following is taken from DOE M 470.4-3A.

Each instructor must possess the skills and knowledge necessary to instruct PF personnel in the requirements for protecting S&S interests. Persons assigned as full-time staff PF instructors must have completed the NTC-certified basic SPO/TRF training program or equivalent training and either must have performed DOE PF-related duties or received site, facility, or organizational on-the-job familiarization with the duties performed by personnel they will instruct. All such training/familiarization must be completed within one year of being assigned to instructor duties. Instructors must demonstrate knowledge of the responsibilities identified in the JA and proficiency in the skills and abilities necessary to perform the associated jobs. These include, but are not limited to, the following:

- Knowledge of teaching methods and instructional techniques
- Knowledge of assigned subject/topical areas for the level of instruction delivered
- Ability to develop course objectives, lesson plans, training aids, and student evaluations
- Skill in presenting a complete instructional lesson plan/course

All PF personnel who are assigned instructor duties must have current certification to the level of training delivered. At a minimum, each instructor assigned to deliver training must successfully complete the DOE NTC basic instructor training course, as approved by the Office of Health, Safety and Security, or an equivalent recognized basic instructor course.

To maintain certification, instructors must conduct at least two classes or two course iterations, or a combination of both, per calendar year. Documentation of these activities must be maintained in the individual's training record. PF management must ensure that each instructor is evaluated for competency at least once every 36 months.

29. Safeguards and security personnel with the responsibility for PFO must demonstrate a working level knowledge of security helicopter flight operations.

a. Discuss the purpose of an Aviation Implementation Plan.

The following is taken from DOE M 470.4-3A.

Helicopters employed in support of security operations provide an airborne dimension to response force capabilities against a threat posed by adversaries who may attempt theft or sabotage of nuclear weapons or SNM and/or sabotage of vital facilities and equipment. The decision to use security helicopters is based on site-specific considerations with concurrence of the cognizant DOE organization or administrator, NNSA. Requirements for helicopter operations are covered in DOE O 440.2B chg 1. Site-specific security helicopter operational mission requirements must be documented in a site-specific aviation implementation plan (AIP). The AIP must be approved by the DOE CSA.

b. Discuss the mission readiness requirements and operations of security helicopters.

The following is taken from DOE M 470.4-3A.

Mission Readiness

To meet mission requirements, a security helicopter must be fully operational and ready to respond to a security emergency with a 90 percent availability rate, excluding weather conditions.

Operations

During a security incident, helicopters may be employed to transport, insert, and relocate response forces to and from the scene of a security incident or staging area as directed by the senior on-scene commander and/or by standard operating procedures. Additional emergency response functions must be fully documented in an AIP and may include, but are not limited to: directed fire; command, control, communications; surveillance; resupply; and support of facility/site protection strategies including recapture, recovery, and fresh pursuit operations.

c. Discuss the conditions and rules of engagement if a helicopter is used as a firing platform.

The following is taken from DOE M 470.4-3A.

Firing from a helicopter can be a viable and effective means of supporting security operations, and the AIP may incorporate aerial firing under the following conditions:

- Authority to include aerial firing in response plans must be granted only following development of site-specific ROE that are consistent with DOE policy on the use of force.

- Firing must be done only by specifically trained and qualified SRT personnel with weapons attached to gun mounts that provide field-of-fire limitations which protect the aircraft from self-inflicted damage.
- A safety analysis review (SAR) of aerial firing must be completed. The SAR must be reviewed for currency any time aerial firing requirements are changed, but at least every twelve months.
- The technical and operational procedures and SAR for aerial firing must be submitted in writing to the cognizant DOE safety officer for approval.
- DOE line management is the final approval authority at each site. Copies of the approved technical and operational procedures for aerial firing must be provided to the senior DOE aviation management official; the cognizant departmental element or the administrator, NNSA; and the Office of Health, Safety and Security.
- Contractor site-specific aerial firing qualification and/or familiarization courses must be developed and submitted, through the DOE CSA to the Chief Health, Safety and Security Officer for review and approval.

d. Discuss the requirement for, and contents of, a Safety Analysis Review (SAR) of aerial firing.

The following is taken from DOE M 470.4-3A.

An SAR of aerial firing must be completed. The SAR must be reviewed for currency any time aerial firing requirements are changed, but at least every 12 months. The technical and operational procedures and SAR for aerial firing must be submitted in writing to the cognizant DOE safety officer for approval.

30. Safeguards and security personnel with the responsibility for PFO must demonstrate a working level knowledge of PFs' equipment and facilities.

a. Discuss the types and quantity of equipment and facilities provided to PFs to effectively and efficiently conduct routine and emergency operations to meet the GSP Policy.

The following is taken from DOE M 470.4-3A.

Equipment

PFs must be equipped and provided with the necessary resources to effectively, efficiently, and safely perform both routine and emergency duties in daylight or under reduced visibility conditions. Equipment, specifically weapons and communications systems, must be tailored to effectively combat and defeat adversaries identified in the GSP and site-specific threat guidance or as specified in the SSP under all environmental and tactical conditions. Equipment must be available in sufficient quantities and properly maintained to support the PF mission.

Facilities

Permanent (routine and emergency duty) PF posts that control access to TRF facilities must meet the following requirements:

- Access control posts must be located so the likely routes of adversary ingress and egress are clearly observable and protected routes or methods of approach are available to PF personnel.
- Fighting positions must be constructed consistent with the VA as documented in the SSP.
- The posts must provide adequate human engineering.
- Exterior walls, windows, and doors must be constructed to meet requirements of DOE M 470.4-2A.
- Lighting must comply with requirements of DOE M 470.4-2A.
- Where automated gates are used to control vehicular access to a security area, the gates and openings must meet the requirements of DOE M 470.4-2A.

Training facilities:

- Suitable facilities to support applicable PF activities must be provided and maintained based on mission-specific needs.
- Training facilities must support realistic, high-intensity PF training and qualification programs. This includes facilities for weapons and physical fitness training, qualifications, and maintenance, special skills, and mission-specific training and qualifications.
- Local, state, and Federal LEAs and DoD/National Guard training facilities are acceptable alternatives to DOE-owned facilities as long as required DOE certifications and safety guidelines are maintained. In coordination with the PF contractor, a memorandum of understanding (MOU) delineating such use must be completed by the DOE CSA and approved by DOE line management.

31. Safeguards and security personnel with the responsibility for PFO must demonstrate a working level knowledge of PF performance testing.

a. Define and discuss the purpose and frequency of the following:

- **Limited Scope Performance Tests (LSPT)**
- **Alarm Response and Assessment Performance Tests (ARAPT)**
- **Validation Force-on-Force (VFoF)**
- **Command Post Exercise (CPX)**
- **Command Field Exercise (CFX)**
- **Joint Training Exercise (JTX)**

The following is taken from DOE M 470.4-3A.

Limited Scope Performance Tests (LSPT)

LSPTs will be either scheduled or unannounced. The tests must be used to determine the level of PF skill or capability or to verify different elements of the PF program. LSPTs must

be conducted to realistically test any operation or procedure, verify the performance of a policy requirement, or verify possession of a requisite knowledge or skill to perform a specific task that falls within the scope of PF responsibility.

Alarm Response and Assessment Performance Tests (ARAPT)

An ARAPT is conducted with no prior notice to evaluate PF response to a specific location under alarm protection, (e.g., a building, vault/CA, or other area that has a site-specific security interest identified in the SSP). The purpose of these tests is to evaluate PF readiness and response to alarm conditions.

These tests must consider all aspects of response including communications, personal protective measures, equipment availability and serviceability, and any PF and facility coordination activities that may be necessary to mitigate a security incident. ARAPTs must be coordinated with FRs and trusted agents to ensure that safety requirements are fulfilled, security is not initiated, and responding PF personnel must be advised of the test. Handguns must be holstered, and any auxiliary weapon must not have a round in the chamber.

Validation Force-on-Force (VFoF)

A VFoF exercise is a major test of the overall effectiveness of all elements involved in response to a GSP and site-specific threats and is used also to validate site-specific protection strategies. VFoF exercises must be held at all facilities having an armed PF annually (at least every twelve months).

Command Post Exercise (CPX)

A CPX is conducted to observe and evaluate a crisis management team's overall handling of simulated safeguards and/or security event or a natural disaster incident. A CPX may involve a local emergency operations center (EOC) or multiple centers including the DOE HQ EOC.

CPXs may be either announced or unannounced and may vary in scope and time as dictated by the purpose of the exercise. A security-related CPX must be based on the GSP and the site-specific threat. The CPX must be used to evaluate both tactical and technical assessments and decisions.

Command Field Exercise (CFX)

A CFX is an extension of a CPX and is conducted to test the interaction among various support organizations, site management, and the PF to a simulated incident. Procedures, tactical intelligence, communications, logistics, and the interfaces between Federal and contractor support systems must be tested during a CFX. Such exercises must be planned and announced in advance to all participating personnel. They may be combined with FoF exercises.

Joint Training Exercise (JTX)

When a VA or PT indicates a need for outside agency support for the successful mitigation of a security incident and such support is properly documented in the SSP, the support expected

from outside agencies must be covered by a formal cooperative agreement, (e.g., MOU). JTXs must be conducted annually (at least every 12 months) and consist of an FoF, CPX, or emergency management exercise with these agencies to determine the agencies' abilities and capabilities to respond to site threats as documented in the SSP and agreed to in the cooperative agreement.

Table 1. Testing Frequency

Type of Performance Test	Minimum Performance Test Frequency
LSPT	At TRF facilities, LSPTs are conducted weekly. At all other facilities conducted as required.
ARAPT	TRF facilities: two/quarter/alarmed SNM locations and one/quarter at all other locations. All other facilities: one/quarter at all alarmed locations.
VFoF	One/year for all sites with armed PFs (additional requirements for category I facilities are contained in DOE M 470.4-1.
CPX	TRF facilities: one/year/site. All other facilities: one/year/site.
CFX	TRF facilities: one/year/site. All other facilities: one/year/site.
JTX	As required per SSP, one/year/site, as applicable.

Note: Annual requirements for VFoF, CPX, CFX, and JTX exercises may be combined when determined appropriate in SSPs. Requirements for ARAPTs may be satisfied through combined testing of multiple alarms in the same or proximate locations and required monthly PF shift and SPO-III shift training exercises.
Source: DOE M 470.4-3A

b. Discuss the five major types of Engagement Simulations Systems (ESS).

The following is taken from DOE M 470.4-3A.

There are six major types of ESS used within DOE for the conduct of simulated engagements during PF PTs and training activities. They are:

- MILES consist of weapons-mounted laser transmitters and harness-mounted laser sensors placed on potential targets to enable accurate and realistic assessment of the effects of PF and adversary weapons fire. Examples of MILES are: handguns, rifles, machine guns, light anti-tank weapons, and claymore mines. MILES are primarily used during PF FoF exercises and LSPTs.
- Marking systems such as: DMC systems consist of modified duty handguns, submachine guns, and rifles and non-lethal DMCs designed to allow for realistic decisional shooting situations during PF PTs and training activities and paint ball (PB) systems consisting of paint guns, also called "markers," that come in a variety of shapes and styles. DMCs and PB rounds have very limited effective and maximum

ranges. Thus, both systems are used typically during LSPTs and training activities to simulate close quarters battle and decision shooting situations.

- Hybrid dye-marking cartridge/ESS firearm is a firearm that has been modified or designated by a DOE-certified armorer as a DMC weapon that feeds, fires, and functions DMC ammunition. The modification reduces the ability for a live round to chamber in the weapon. The weapon is mounted with a MILES transmitter.
- Blank-fire equipment consists of specially modified duty firearms and blank-fire cartridges designed to provide realism during PTs and PF training on the use of deadly force and the escalation of the force continuum.
- Inert weapons systems consist of simulated firearms and weapons or actual firearms and weapons that have been rendered incapable of firing live or blank-fire ammunition. Inert weapons systems are typically used to simulate firearms and weapons during PF control and restraint training and LSPTs.
- Airsoft systems, sometimes referred to as soft air systems, consist of replica duty weapons that propel 6mm plastic or biodegradable ball bearings (BBs) by means of either rechargeable batteries or Green Gas (HFC 143a). This system can also be modified to be used with the ESS equipment without the use of BBs. Airsoft weapons training systems can be used in virtually any work area. They will not accept live or blank rounds.

c. Discuss the safety factors and rules of engagement involved with the deployment of ESS.

The following is taken from DOE M 470.4-3A.

Safety

Safety is a major concern in any ESS PT, and training activity and safety rules must be followed to minimize the potential for accidents/injuries during these activities. Management, controllers, and participants must caution and prepare participants to anticipate and react to unsafe situations. Realism must be achieved and safety must be considered in the actions of all participating personnel. Preparations must also be made to react with appropriate levels of medical assistance to situations that could occur. See DOE M 470.4-3A, attachment 1, appendix B, for more safety rules.

Rules of Engagement

An ESS PT or training activity may be halted at any time for safety, emergency, real-time security events, or administrative reasons. An exercise freeze is a command that is used to halt an exercise when it is necessary to correct safety-related problems or respond to an emergency.

The command “administrative hold” is used to halt an ESS PT when it is necessary to correct exercise problems of an administrative or procedural nature. The use of the command may be planned when it is necessary to put a temporary hold on activities to set the stage for continuation of the PT (e.g., change scenarios, operations shift change activities, etc.).

All pre-exercise actions must be conducted according to normal operating procedures. Participants must be closely monitored to ensure they do not use artificially generated factors to affect the outcome of the PT. Participants must be familiar with the operation of issued ESS equipment. Participants who will be using or handling pyrotechnics, diversionary devices, hazardous materials, or electrical or mechanical equipment must receive training in their proper use according to current applicable requirements.

Before being assigned to act as hostages/role players, individuals must be asked if they are willing and capable of dealing with the isolation and demands of a hostage/barricade situation.

d. Demonstrate the ability to assess the contractor's performance test plans involving ESS; examining the activity, command and control, and safety as applicable to S&S planning principles.

This is a performance based KSA. The Qualifying Official will evaluate its completion.

e. Discuss the use of the computer modeling Joint Conflict and Tactical Simulation (JCATS) and tabletop modeling Analytic System and Software for Evaluating Safeguards and Security (ASSESS) to evaluate PFO.

Joint Conflict and Tactical Simulation (JCATS)

The following is taken from U.S. Joint Forces Command (USJFCOM) Fact Sheet, *Joint Conflict and Tactical Simulation*.

The JCATS program is an interactive simulation tool sponsored by USJFCOM and managed from the command's Joint Warfighting Center in Suffolk, VA.

The military uses JCATS for training, analysis, and mission planning and rehearsal. JCATS simulates operations in urban terrain, supports non-lethal as well as conventional weapons, and allows users to quickly assemble and disband entities and units. JCATS provides a wide range of operations in a variety of dynamic simulated environments. The simulation models the dynamics of individual soldiers, vehicles, and weapons, increasing the realism of the simulation and allowing for more direct participation. Both the Army and the Marine Corps use the simulation for training and real-world rehearsals of tactical missions.

Numerous units used the simulation for tactical training prior to deploying in support of Operation Iraqi Freedom, both as a stand-alone simulation, and with live, virtual, and constructive simulation as part of the Joint National Training Capability enhancements. JCATS also provides the high-resolution support for homeland security for U.S. Northern Command training events as part of the Joint Multi-Resolution Model Federation with the joint theater level simulation program

Analytic System and Software for Evaluating Safeguards and Security (ASSESS)

The following is taken from A Risk Assessment Methodology (RAM) for Physical Security, by Sandia Laboratory.

Analysis and evaluation of the security system begin with a review and thorough understanding of the protection objectives and security environment. Analysis can be performed by simply checking for required features of a security system, such as intrusion detection, entry control, access delay, response communications, and a response force. However, a security system based on required features cannot be expected to lead to a high-performance system unless those features, when used together, are sufficient to ensure adequate levels of protection. More sophisticated analysis and evaluation techniques can be used to estimate the minimum performance levels achieved by a security system.

The adversary sequence diagram (ASD) is a graphical representation of physical protection system elements along paths that adversaries can follow to accomplish their objective. For a specific physical protection system and threat, the most vulnerable path can be determined. This path with the least physical protection system effectiveness establishes the effectiveness of the total physical protection system. An ASD is developed for a single critical asset associated with an undesired event. Computer codes such as Systematic Analysis of Vulnerability to Intrusion (SAVI) and ASSESS can be used to determine the most vulnerable path. The neutralization module of ASSESS or JCATS can be used to estimate response force effectiveness.

D. INFORMATION PROTECTION (IP)

Competencies and supporting knowledge and skills for section D, Information Protection, are derived from the following DOE Orders, manuals, and guides:

- 10 CFR 1016, "Safeguarding of Restricted Data"
- 32 CFR 2003, "National Security Information-Standard Forms"
- DOE O 470.4A, *Safeguards and Security Program*
- DOE M 470.4-4A, *Information Security Manual*

32. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the security requirements for the protection and control of information and matter required to be classified or controlled by statues, regulations, or DOE directives.

a. Discuss the requirements for the planning and implementation of a CMPC Program.

The following is taken from DOE M 470.4-4A.

To ensure the protection and control of classified information and matter, a classified matter protection and control (CMPC) program must be implemented to cover each departmental element, site, and/or facility and must be tailored to achieve the protection levels that adequately address specific site characteristics and requirements, current technology, ongoing programs, and operations needs.

The CMPC program, in addition to ensuring compliance with the requirements of DOE M 470.4-4A, must also include the following activities:

- Establishment of a point of contact with overall CMPC responsibilities for each site, facility, and program office.
- CMPC point(s) of contact must ensure that the content of local CMPC training and/or briefings and awareness is commensurate with personnel responsibilities in support of the CMPC program.
- Promulgation of CMPC requirements to all affected employees.

Protection Strategies and Planning:

- Strategies for the protection and control of classified matter must incorporate the applicable requirements established in DOE M 470.4-4A.
- The level of protection and resources expended on CMPC programs must be commensurate with their required effect on deterring or detecting compromise of or unauthorized access to classified matter. Protection measures should provide a graded approach, identifying each layer of protection between the adversary and the asset.
- S&S plans. The details of site protection measures for classified matter must be described in the applicable SSP (see DOE M 470.4-1 chg 1).

b. Discuss the training requirements for the CMPC Program.

The following is taken from DOE M 470.4-4A.

All CMPC-related training/briefing regarding the local implementation of DOE M 470.4-4A must be formally documented. It must also be approved by the CSA (e.g., frequency, content). (Specific training requirements, in addition to those stated below, are included in DOE M 470.4-1.)

- Each individual identified as a CMPC point of contact, according to DOE M 470.4-4A, section A, chapter I, paragraph 1.b, must receive initial training within one year of appointment or as soon as training is available through the NTC. Other personnel may also receive the NTC-developed training.
- All personnel with security clearances whose classified matter responsibilities include access (potential or actual), originating, handling, using, storing, accounting for, reproducing, transmitting (including hand-carrying), destroying, and/or emergency reporting must receive CMPC training and/or briefings commensurate with these responsibilities prior to receiving access to classified matter and receive refresher training and/or briefings to ensure continued reinforcement of requirements. This training and/or briefing must be tailored to the assigned duties and responsibilities of the persons receiving the training and/or briefing.

- Personnel with security clearances whose job responsibilities do not meet the conditions specified in DOE M 470.4-4A, section A, page I-5, paragraph 4.b, (e.g., personnel employed in maintenance, janitorial, food service, and other such activities) must receive training and/or briefings and be able to identify unprotected classified matter (e.g., by classified cover sheets and classification markings) and know the associated reporting requirements.

c. Describe the storage requirements that apply to security containers, vaults, or vault-type rooms (VTRs) that contain classified matter or other S&S interests. [Note: Vault type rooms (VTRs) has been replaced with the term closed areas (CAs). Ref: NAP-70.4]

The following is taken from DOE M 470.4-4A.

The following PS storage requirements apply to classified S&S interests.

Repositories used to store classified matter must not be used to store or contain other items that may be a substantial target for theft.

Security containers used for storing classified matter must conform to GSA standards and specifications. All GSA-approved security containers must be maintained within limited or higher security areas unless otherwise noted in DOE M 470.4-4A. Vaults and CAs used for open storage of classified matter must meet the requirements of DOE M 470.4-2A. Classified matter that is not under the personal control of an individual with appropriate security clearance and need-to-know must be stored as described below:

- If inspections by PF personnel are used as supplemental control, PF personnel must examine exposed surfaces of the secure storage repositories and steel filing cabinets for evidence of any forced entry to ensure that the security container or door is locked and the SF 702 completely annotated.
- Areas and buildings must be protected from adversary access by application of GSA-approved locks and barriers. Requirements for these locks and barriers can be found in DOE M 470.4-2A.

Confidential matter must be stored in the same manner prescribed for S or TS matter, but the supplemental controls are not required.

Secret matter must be stored as described below or in any manner authorized for TS matter.

- In a locked vault or in a locked GSA-approved security container within an LA or higher.
- In a locked CA within an LA, EA, PA, or MAA equipped with IDS protection. PF personnel must respond within thirty minutes of alarm annunciation.
- When locked outside an LA, the locked vault or CA must be under IDS protection. PF personnel must respond within fifteen minutes of alarm annunciation.
- In locked, steel filing cabinets that do not meet GSA requirements and are equipped with three-position, dial-type, and changeable combination locks. The cabinet must

be in a locked area or building within the minimum of an LA. In addition, one of the following supplemental controls is required:
  - Intrusion detection system protection that provides for response from PF personnel within thirty minutes of alarm annunciation
  - Inspection every four hours by PF or by cleared duty personnel when unattended

Top Secret matter must be stored as described below:

- In a locked, GSA-approved security container with one of the following supplemental controls:
  - Under IDS protection and by PF personnel responding within fifteen minutes of alarm annunciation
  - Inspection by PF personnel no less frequently than every two hours
- In a locked vault or CA within an LA, EA, PA, or MAA. The vault or CA must be equipped with intrusion detection equipment, and PF personnel must respond within fifteen minutes of alarm annunciation.
- In a locked vault or CA within a PPA or outside of a security area, under IDS protection. PF personnel must respond within five minutes of alarm annunciation.

d. Discuss the policies and procedures for the documentation requirements that must be met for each security container, vault, or VTR approved to store classified matter. [Note: The term vault type room (VTR) has been replaced with the term closed areas (CAs). Ref: NAP-70.4]

The following is taken from DOE M 470.4-4A.

Documentation—SF 700, *Security Container Information*, part 1 must be completed for each secure storage repository or other locations approved for storing classified matter and include the names of all individuals who may be contacted if the container is found open and unattended. A record must be maintained of all individuals who have or may be granted access to the secure storage repository combination.

- The local implementation plan may dictate whether or not block 8, *Serial No. of Lock*, must be left blank.
- SF 700, part 1, must be affixed to the inside of the door of vaults and CAs containing the combination lock. For security containers, it must be placed inside the locking drawer.

SF 700, part 2a must be used to document the combination of the secure storage repository. It must be marked front and back with the highest level and most restrictive category (if RD or FRD) of information that may be stored within the repository and inserted in the accompanying envelope (part 2).

SF 700, part 2 (envelope) must be marked front and back with the highest level and most restrictive category (if RD or FRD) of information that may be stored within the secure storage repository. Once completed and sealed, it must be forwarded to central records for storage that prevents access by any individual who does not possess the same security

clearance, any required formal access approval, and need-to-know. If the combination protects information requiring additional access approval (e.g., Sigma 14, Sigma 15, North Atlantic Treaty Organization (NATO), SAP information, or SCI), the part 2 must not be sent to central records unless all individuals at that location possess the same security clearance, any required formal access approval, and need-to-know.

SF 701, *Activity Security Check List*. The SF 701 provides a systematic means of checking end-of-day activities for a particular work area, allowing for employee accountability in the event that irregularities are discovered. Use of SF 701 is optional except when local security and/or implementation plans require its use for detailed end-of-day security inspections.

SF 702, *Security Container Check Sheet*:

- The SF 702 must be used to record security checks each day a container may have been accessed by documenting the times and the initials of the person(s) who has opened, closed, or checked a particular container, room, vault, or CA holding classified information.
- The SF 702 must be used for any secure storage repository used to store accountable classified removable electronic media (ACREM), including locked drawers or file cabinets in vaults and CAs and those that use XO-series locks.
- The SF 702 must be in a conspicuous location and affixed or in proximity to each security container and/or the entrance to each vault or CA.

e. Discuss the requirements for classifying and protecting combinations for containers that store classified matter.

The following is taken from DOE M 470.4-4A.

Combinations to containers containing ACREM must be limited to the responsible ACREM primary and alternate ACREM custodian(s). When there are multiple shifts, the combination can be provided to the ACREM primary and alternate ACREM custodian(s) for each shift. A designated individual may be provided the combination only when the ACREM primary and all alternate ACREM custodian(s) are not available and access is required.

Combinations must be changed by an appropriately cleared and authorized individual as soon as possible after any of the following situations occur.

- Initial receipt of a GSA-approved security container or lock.
- When an individual who knows the combination is reassigned, transferred or terminated; has his/her security clearance downgraded to a level lower than the level of classified matter stored; or has his/her security clearance administratively terminated or suspended.
- Maintenance is performed by a locksmith or safe technician.
- When the ACREM custodian(s) and/or alternate ACREM custodian(s) return after the combination has been provided to the designated individual.
- Compromise or suspected compromise of security storage repository.

- Preparation for turning in a completely empty security container. The combination must be set to factory standard 50-25-50 before the container is turned in. When a security container is transferred from one organization to another, the custodian from the original organization must certify, in writing, that all classified matter has been removed before the transfer takes place.
- Combinations used to protect NATO material must be changed no less frequently than at twelve-month intervals.

Combination numbers must be selected at random. Security containers with multiple locking drawers must contain a classified combination on each drawer.

33. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for CMPC.

a. Discuss the CMPC requirements.

The following is taken from DOE M 470.4-4A.

To ensure the protection and control of classified information and matter, a CMPC program must be implemented to cover each departmental element, site, and/or facility and must be tailored to achieve the protection levels that adequately address specific site characteristics and requirements, current technology, ongoing programs, and operational needs.

The CMPC program, in addition to ensuring compliance with the requirements of DOE M 470.4-4A, must also include the following activities:

- Establishment of a point of contact with overall CMPC responsibilities for each site, facility, and program office.
- CMPC point(s) of contact must ensure the content of local CMPC training and/or briefings and awareness is commensurate with personnel responsibilities in support of the CMPC program.
- Promulgation of CMPC requirements to all affected employees.

b Discuss the requirements for the use of a cover sheet for a document undergoing classification review.

The following is taken from DOE M 470.4-4A.

When matter must be sent outside the office of origin for a classification and determination, it must be marked "DRAFT—Not Reviewed for Classification." To preclude marking every page of a document being transmitted for classification review, it should have a "Document Undergoing Classification Review" cover sheet that is marked with the highest level and most restrictive category of information the originator believes is contained in the document.

c. Discuss the policies and procedures pertaining to access to classified matter in an emergency.

The following is taken from DOE M 470.4-4A.

Access to classified matter in an emergency involving an imminent threat (explosion, fire, etc.) to life or defense of the homeland may be provided to individuals who are not otherwise routinely eligible for access to classified matter. If an emergency is life-threatening, the health and safety of individuals takes precedence over the need to protect classified matter from disclosure. Examples of such releases including providing law enforcement personnel with classified information concerning an improvised nuclear device found in a public place, sharing a classified DOE evaluation of the viability of a nuclear threat message with local emergency response personnel, or providing an attending physician with classified details about nuclear materials at a site to assist in the emergency treatment of a patient.

d. Discuss the policies and procedures pertaining to protection and control of classified matter that is in use.

The following is taken from DOE M 470.4-4A.

Classified matter in use must be constantly attended by or under the control of a person possessing the proper security clearance and need-to-know. Physical control must be maintained over any matter marked as containing C/FGI-MOD matter to prevent unauthorized access to the information.

e. Discuss the policies and procedures pertaining to protection and control of classified matter that is in storage, including non-conforming storage.

The following is taken from DOE M 470.4-4A.

Classified matter must be stored under conditions designed to deter and detect unauthorized access to the matter, to include securing it in approved equipment and facilities whenever it is not under the direct control of an authorized person. Non-conforming storage may only be used for classified matter and cannot be protected by the established standards and requirements due to its size, nature, operational necessity, or other factors. In these exceptional cases, non-conforming storage that deters and detects unauthorized access to the classified matter may be used for storing classified matter.

Non-conforming storage must result in protection effectiveness equivalent to that provided to similar level(s) and categories of classified matter by standard configurations. The methods, protection measures, and procedures must be documented and approved by the DOE CSA. Documentation must include the following:

- Explanation as to why exercising this option is necessary
- Description of classified matter to be stored
- Description of the means by which equivalent security is to be provided
- An analysis demonstrating the equivalence of protection

- A copy of the documentation must be maintained locally
- Copies of the documentation must be forwarded to the cognizant headquarters departmental element
- Updates to this documentation as conditions change

Burial is an option that may be approved by the DOE CSA for permanent placement of classified matter. In addition to meeting the requirements for non-conforming storage of classified matter, permanent burial documentation must also include the following:

- For active burial operations, description of the entire placement process, including protection of classified matter prior to final burial
- Configuration of classified matter to be buried
- Assurance that undisturbed burial is designed and will be sustained indefinitely for the buried classified matter
- Explanation of current and future use of the burial location and all pertinent location characteristics (natural or engineered) that will limit or preclude access to the classified matter
- Updates to this documentation as conditions change

Classified matter that is accountable is considered to meet accountability requirements when it is permanently placed into an approved burial configuration. Inventory of previously accountable classified matter may be suspended indefinitely as long as there has been no access to the matter since it was buried.

f. Discuss the policies and procedures pertaining to protection and control of classified matter that is being transmitted and received.

The following is taken from DOE M 470.4-4A.

Classified matter must be transmitted only in the performance of official or contractual duties. If the transmission is not required by the specific terms of the contract or required for performance of the contract, contractors must obtain written authorization from the DOE CSA before transmitting classified matter outside the facility. Before transmitting classified matter, the sender must ensure the following:

- The recipient has the appropriate security clearance, has any required programmatic or special access approval, and meets the need-to-know criteria.
- An approved classified address has been identified and used for the appropriate method of transmission, (e.g., mailing, shipping, or overnight delivery).

When classified matter is received at a facility, the following controls must apply:

- Classified matter must be delivered to personnel designated to receive it at a control station with the inner envelope unopened. Procedures must be established to ensure that when classified matter is not received directly by the designated control station (regardless of the type of mail system), the inner container remains unopened.
- The package must be examined for evidence of tampering and the classified contents checked against the receipt (if provided). Evidence of tampering must be maintained

and reported promptly to the CSA. If the matter was received through the U.S. Postal Service, the appropriate U.S. Postal Inspector must also be notified promptly. Discrepancies in the contents of a package must be reported immediately to the sender. If the package (or container) is in order and includes a receipt, the receipt must be signed and returned to the sender.

g. Discuss the policies and procedures pertaining to accountability of classified matter.

The following is taken from DOE M 470.4-4A.

Control systems must be established and used to prevent unauthorized access to or removal of classified information. Accountability systems must provide a system of procedures that provide an audit trail. Accountability as defined below, applies regardless of the physical form of the matter. Accountability procedures must be approved by the CSA.

The material accountability system must provide a description of each type of item, the classification level and category (if RD or FRD), the number of items of each type, and scheduled inventories. Part numbers and serial number should be used, when available, as a unique number or to identify the types of material. When applicable, the production cycle and production control procedures can be used to facilitate the conduct of all inventories of accountable material.

Control stations must be established to maintain records, accountability systems, access lists, and to control classified matter (including facsimiles) received by and/or dispatched from facilities. Control station operators must maintain accountability systems for accountable matter. A defined and operated ACREM accountability process may function as a control station.

Accountability records are required when accountable matter is originated, reproduced, transmitted, received, destroyed, permanently buried, or changed in classification. All sites must develop procedures to ensure that all accountable matter has been entered into accountability systems.

34. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for marking classified matter.

a. Discuss the requirements for the marking of classified matter.

The following is taken from DOE M 470.4-4A.

All classified matter, regardless of level and category, must be marked to ensure information is appropriately protected to prevent inadvertent disclosure. Classified matter must be reviewed and brought up to current marking standards whenever it is released by the current

holder ("current holder" may be defined as an individual, specific office, or ad-hoc working group [AHWG]) or removed from archival storage.

Classified matter, regardless of date or agency of origin must be marked to indicate at least the classification level and category. All classification markings must be distinguishable from the document text. The overall classification level (i.e., TS, S, or C) of a document must be marked on the top and bottom of the cover page (if any), the title page (if any), the first page of text, and the outside of the back cover or last page of text. The classification level and category (if RD or FRD) must be clearly marked on all other (non-document) classified matter if possible. Otherwise, alternative marking methods must be used to identify the overall classification level and category (if RD or FRD). When marking the level or category is not practical, written notification must be furnished to all recipients. The originator is responsible for ensuring that classified matter is marked according to DOE M 470.4-4A. DOE M 475.1-1B, *Manual for Identifying Classified Information*, contains additional marking requirements beyond the requirements contained in DOE M 470.4-4A.

All interior pages of documents must be marked top and bottom with either: the overall classification level and category (if RD or FRD) for the entire document, or the highest classification level and category (if RD or FRD) of all information on that page; or with the appropriate unclassified marking if there is no classified information on that page.

b. Discuss the requirement for the proper identification of the originating organization, date, and classification level on all classified matter.

The following is taken from DOE M 470.4-4A.

The name and address of the organization responsible for preparing the document and the date of preparation must appear on the first page of all classified documents.

c. Discuss the marking of classified matter with the assigned classification level and category.

The following is taken from DOE M 470.4-4A.

The three classification categories are RD, FRD, and NSI. Classified matter containing only NSI is not marked with an NSI admonishment.

- If the document contains RD or FRD information, the appropriate admonishment information must be marked on the first page of the document, whether cover page, title page, or first page of text and appear in the lower left corner.
- RD or FRD documents generated prior to July 9, 1998, are not required to be re-marked to indicate the category on each page containing RD or FRD information unless they are sent outside the office of origin or holder for other than archiving purposes.

d. Discuss the requirements for marking classified matter that has mixed levels and categories.

The following is taken from DOE M 470.4-4A.

When classified matter contains a mix of information at various levels and categories that causes the document to be marked at an overall level and category higher than the protection level required for any of the individual portions, a marking matrix may be used in addition to other required markings. This would allow an individual with a lower access level, such as an "L" cleared employee, to be given access to a document that they might not otherwise have been authorized access to if the document was only marked at the highest overall classification level and category. (For example, a document that contains C/RD and S/NSI would be required to be marked as S/RD, the highest level and most restrictive category. None of the information in the document is S/RD.) However, this may not be interpreted to authorize any individual to gain access to information that exceeds their security clearance, formal access approvals, and need-to-know.

If the marking matrix is used, the following marking, in addition to other required markings, must be placed on the first page of text. The marking should appear on the lower right corner near the classifier information marking. If the derivative classifier places this marking on the document at the time of the classification decision, there is no need to indicate the name and title of the derivative classifier on the mixed level and category marking.

e. Discuss the requirements for marking classified matter that has multiple components that can be used separately.

The following is taken from DOE M 470.4-4A.

When components of a document are to be issued or used separately, each major component must be reviewed and marked as a separate document. Components include annexes or appendices, attachments, and major sections of a report. If an entire major component is unclassified, "Unclassified" must be marked at the top and bottom of the first page and a statement included (e.g., "All portions of this [annex, appendix, etc.] are (U)"). When this method of marking is used, no further markings are required on the unclassified component. Documents transmitted with a letter of transmittal are discussed in DOE M 470.4-4A, section A, paragraph 3.o.

f. Discuss the marking of unclassified matter that is embedded in classified matter.

The following is taken from DOE M 470.4-4A.

Unclassified matter need not be marked unless it is essential to convey one of the following conditions:

- The matter has been reviewed for classification and does not contain classified information; or
- The matter has been properly declassified.

If unclassified matter is marked, the (U) marking must be placed on the top and bottom of the front cover (if any), title page (if any), and first page of text.

g. Discuss the requirements for marking portions of classified documents.

The following is taken from DOE M 470.4-4A.

Portion marking:

- NSI documents dated after April 1, 1997, must be portion marked.
- Documents containing RD or FRD should not be portion marked; however, if portion-marked, markings must be consistent with DOE M 470.4-4A, section A.
- Portion markings must include any applicable caveats. Each section, part, paragraph, graphic, figure, subject/title, or similar portion of any such document must be accurately marked to show
  - the classification level, category (if RD or FRD), and caveat (e.g., S/RD, S/FRD, C/RD, C/FRD, S, TS, S/NOFORM, etc.) or
  - that it is unclassified (e.g. Unclassified Controlled Nuclear Information [UCNI], Official Use Only [OUO], or [U].
- Page changes to NSI documents dated after April 1, 1997, must be portion-marked. Additionally, any NSI document that becomes active (i.e., when it is released by the current holder, which may be defined as an individual, specific office, or AHWG, or removed from archival storage) must be portion marked with the appropriate classification level, caveat, or unclassified.
- Portions of U.S. documents containing FGI must be marked to reflect the foreign country of origin and appropriate classification level (e.g., U.K.-C, indicating United Kingdom-C). Foreign Government Information must be indicated in lieu of the country of origin if the foreign government indicates it does not want to be identified.
- Classification by association or compilation. DOE M 475.1-1B contains portion marking and other requirements for classified matter determined to be classified by association or compilation.

h. Discuss the use and marking of subjects and titles used for classified documents.

The following is taken from DOE M 470.4-4A.

Titles must be marked with the appropriate classification (level; category if RD or FRD; and other applicable caveats) or control symbol or "U" if unclassified and placed immediately after the item.

i. Discuss the policies and procedures for using caveats and special control markings.

The following is taken from DOE M 470.4-4A.

Caveats and special control markings are placed on documents to identify special handling or dissemination requirements or to assist in describing the type of information involved or who distributed or originated the information. Caveats and special control markings and any related admonishment statements or notices should be placed above the category admonishment statement, if any, on the lower left corner of the first page (cover page, if any; title page, if any; or first page of text) and in portion markings, when required.

j. Discuss the policies and procedures for remarking, upgrading, and downgrading classified matter.

The following is taken from DOE M 475.1-1B.

Downgrading/Upgrading

The person changing the classification markings on a document or material based on receipt of a downgrading or upgrading notice must include the following information on the front of the document:

- The appropriate classification level and category (if RD or FRD) on the "Classification changed to" line
- A brief description of the notice advising of the change in classification and its date on the "Authorized by" line (e.g., Change Notice 138, August 31, 2006)
- The name of the person making the change and the date the change is made on the "Changed by" line

In addition, if the downgrading action resulted in a change from the RD/FRD categories to the NSI category, the person making the change must ensure that declassification instructions and portion markings are applied as described in the notification. Note: Adequate quality assurance measures should be in place to ensure that the classification change announced in the notice is done correctly.

k. Discuss the policies and procedures for marking declassified matter.

The following is taken from DOE M 475.1-1B.

Declassified

For each document or material that is declassified, the derivative declassifier crosses out or authorizes the crossing out of the classification markings and provides the following information:

- The names or personal identifiers and positions or titles of individuals declassifying the document for the "Declassified By" line.
- For the "Derived From" line:
  - For DOE-approved guidance, the short title, issuance date of the guide, and "DOE OC"
  - For other-agency guidance, the short title, issuance date of the guide, agency, and where applicable, the office issuing the classification guidance

- If more than one guide was used to declassify the document, enter the words "Multiple Sources" on this line and include a list identifying each guide with the record copy of the document

- The date of declassification for the "Declassified On" line

I. Discuss the policies and procedures for marking the following:

- **Charts, maps, drawings, and tracings**
- **Messages**
- **Classified electronic mail (E-Mail) messages**
- **Facsimiles**
- **Microfiche, microfilm, and aperture cards**
- **Motion picture films and video tapes**
- **Photographs and negative rolls**
- **Transparencies, slides, and sheet film**
- **Magnetic, electronic, or sound recordings**
- **Classified information system media**
- **U.S. classified information translated into a foreign language**
- **Unclassified matter used to simulate or demonstrate classified matter for training purposes**
- **Classified page changes that result from periodic updates to a classified document**
- **File folders and other containers containing classified matter**
- **Working papers**

Charts, Maps, Drawings, and Tracings

The following is taken from DOE M 470.4-4 chg 1 (archived).

When such documents are printed on larger than the standard 8.5-inch by 11-inch sheets, the overall level and category (if RD or FRD) of the document must be marked under the legend, title, or scale block. The classification level and category (if RD or FRD) must be visible when these types of documents are folded or rolled. These types of NSI documents do not require portion-marking unless such markings are determined by the cognizant classification or security authority to be operationally necessary. The unique identification number, if accountable, should be placed either in the upper, right-hand corner or under the legend, title, or scale block. If the chart, map, or drawing is incorporated into a document, it will be marked the same as any other page of the document.

Messages

The following is taken from DOE M 470.4-4 chg 1 (archived).

The overall classification level and category (if RD or FRD) of the message must be the first item of information in the text. When messages are printed by an automated system, markings may be applied by that system provided the markings are clearly distinguishable from the informational text. If applicable, declassification instructions must be included on the last line of text and may be abbreviated as DECL (date, exemption, or event).

Classified Electronic Mail (E-Mail) Messages

The following is taken from DOE M 470.4-4 chg 1 (archived).

Marking of classified e-mail messages:

- Each classified e-mail message must include
  - as the first item of information in the text, the highest level and category of the accredited classified information system or the appropriate markings for the classification of the information as determined by a derivative classifier;
  - name and organization of originator;
  - date of transmission;
  - subject and title marking as required for all classified documents; and
  - any applicable caveats or special handling and dissemination requirements.
- Any attachment to a classified e-mail message must be appropriately marked
  - at the top and bottom of each page with the highest level and category of the accredited classified information system; or
  - as a final document with the appropriate classification of the information as determined by a derivative classifier.
- If the e-mail message or attachment is printed to hard copy, the recipient must ensure it is marked appropriately, either
  - as a working paper; or
  - as a final document by obtaining a classification review by a derivative classifier or, if a derivative classifier is not available at the recipient's location, by having the originator provide a message already reviewed by a derivative classifier and marked in final format.

Facsimiles

The following is taken from DOE M 470.4-4 chg 1 (archived).

A classified document transmitted by an approved classified facsimile machine must be marked, if possible, as a final document before transmission. DOE F 1325.7, *Telecommunication Message*, may be used as the first page of the facsimile. This form or a locally developed form may be marked either as an unclassified letter of transmittal or as the first page of the classified document. When classified drafts are transmitted by facsimile, they should be marked at the highest potential overall classification level and category. When final classification determination is made, the originating agency is responsible for ensuring that all previous recipients receive a correctly marked version with instructions to destroy all previous draft copies.

Microfiche, Microfilm, and Aperture Cards

The following is taken from DOE M 470.4-4 chg 1 (archived).

Each microfiche must be marked either photographically on the film or by using an adhesive label.

- The first and last image of each microfiche should reflect the highest classification level, category (if RD or FRD), and caveats (if applicable) of information contained on the microfiche.
- Declassification instructions (NSI only) should be placed on the microfiche so it is readable with the unaided eye, if such markings would apply to all of the classified information on the microfiche. If it will not fit, the declassification instructions should be placed on accompanying documentation.
- The classification level and category (if RD or FRD) and unique identification number (if accountable) must be placed across the top of the microfiche. The classification level and category (if RD or FRD) must also be placed on the bottom (classification level and category must be readable by the unaided eye).

Each microfilm reel must be marked on its face (i.e., on the reel itself) to reflect the classification level, category (if RD or FRD), caveats (if applicable), and unique identification number (if accountable). Declassification instructions must be placed on the reel, if such markings would apply to all the classified documents on the microfilm. If these instructions will not fit, they must accompany the microfilm (consider placing this information on accompanying documentation).

- Declassification instructions must be placed on the first image, if such instructions would apply to all the classified documents on the microfilm. If the instructions will not fit, they must be placed on accompanying documentation.
- The second image should contain the reel number.
- The third image should contain the reduction ratio used in microfilming the documents.
- The image immediately preceding the end of the reel should contain an index of the documents microfilmed.
- The end of each reel must contain the highest level and category (if RD or FRD) of information on the reel.

Aperture Cards

The following is taken from DOE M 470.4-4 chg 1 (archived).

An aperture card is a punched, automatic data processing card on which a portion of a microfilmed document is mounted. Unclassified aperture cards are off-white and have the upper-left corner cut. S and C images are on reddish stock without cut corners. The difference in color and the cut corner helps distinguish between the classified and unclassified aperture cards when they are commingled and stacked. TS information should not be placed on an aperture card. The classification level should be marked near or above the microfilmed image on the face of the aperture card. The category (if RD or FRD) should be placed below the microfilmed image. If the classification level and category markings cannot be used, this information may be coded on the aperture card. The microfilm image should contain the classifier information, level, and category (if RD or FRD) in reduced size.

Motion Picture Films and Video Tapes

The following is taken from DOE M 470.4-4 chg 1 (archived).

At the beginning of a film or video tape, the following information must be projected for approximately five seconds in the sequence given: classification level, classification category (if RD or FRD), caveats (if applicable), classifier information, and unique identification number (if accountable). At the end of a film or videotape, the classification level and category (if RD or FRD) must be projected for approximately three seconds. The face of the video tape cartridge or the face/side of the film's reel must be marked with the classification level and category (if RD or FRD).

Only the removable covering of a film or tape is considered a container and must be marked according to other containers.

Photographs and Negative Rolls

The following is taken from DOE M 470.4-4 chg 1 (archived).

Classification markings (classification level, category [if RD or FRD], caveats [if applicable], classifier information, and the unique identification number, if accountable) must be applied (if necessary, to the reverse side or affixed by a pressure tape label, staple strip, or other comparable means). When self-processing film or paper is used to photograph or reproduce classified information and all parts of the last exposure have not been removed from the camera, the camera must be protected at the highest classification level and category of information contained on the medium.

Roll negative or positives must be marked at the beginning and end of each strip. The markings at the beginning of a roll must be placed in the following order: classification level, category (if RD or FRD), caveats (if applicable), classifier information, and the unique identification number (if accountable). The markings at the end of the roll must have the classification level and category (if RD or FRD). Note: Any rolls created prior to publication of DOE M 470.4-4 chg 1 may be marked according to the marking requirements in place at the time the roll was originated. Copies of such previously created rolls must be marked according to current requirements.

Transparencies, Slides, and Sheet Film

The following is taken from DOE M 470.4-4 chg 1 (archived).

The overall classification level, category (if RD or FRD), and any caveats must be shown on the image of the first transparency, slide, or sheet film of a series. All other applicable markings specified in DOE M 470.4-4 chg 1, (archived), section A. must be shown on the border or the frame or in the accompanying documentation. The succeeding transparencies, slides, and sheet film must indicate the classification level and category (if RD or FRD) on the image.

When individual pages in a set of transparencies, slides, or sheet film are to be handled and controlled as separate documents, each page requires all standard markings. Each transparency, slide, or sheet film may be regarded as an individual portion and does not require further portion marking.

Magnetic, Electronic, or Sound Recordings

The following is taken from DOE M 470.4-4 chg 1 (archived).

Magnetic, electronic, or sound recordings must indicate the overall classification level, category (if RD or FRD), and applicable caveats at the beginning and end of the recording. The classification level, category (if RD or FRD), caveats (if applicable), unique identification number (if accountable), and classifier information must be applied to the face of the recording by adhesive tape or similar material.

Classified Information Systems Media

The following is taken from DOE M 470.4-4 chg 1 (archived).

All classified information systems media must be marked with the accreditation level of the information system unless an appropriate classification review has been conducted. All classified electronic storage media (ESM) must have the overall classification level and category (if RD or FRD) visible on the front and back. Media may be marked using a standard form (SF 710 for unclassified, SF 709 for classified, SF 708 for C), SF 702 for S, and SF 706 for TS) (see http://www.archives.gov/isoo/security-forms/) or locally developed labels required on the exterior of ESM. Only the removable covering of classified ESM is considered a container and must be marked according to DOE M 470.4-4 chg 1, paragraph 3.q.

- If a platen or disk is removed from its manufacturer's case and is not immediately destroyed, it must be marked with the classification level and category (if RD or FRD).
- Levels that denote the classification level and category (if RD or FRD) of the media may be used when it is practical to apply the label without impeding the operation of the removable media.
- If the label can impede the operation of the removable media, (e.g., not allowing the media to properly seat), alternative marking methods are required.
- The classification markings must be visible and human-readable, and must easily communicate the classification level and category (if RD or FRD) of the information.

U.S. Classified Information Translated Into a Foreign Language

The following is taken from DOE M 470.4-4 chg 1 (archived).

U.S. classified information translated into a foreign language must be marked as U.S. classified information and must show the equivalent foreign government classification (see table below).

Table 2. Foreign equivalent classification markings

Country	Top Secret	Secret	Confidential	Confidential FGI-Modified Handling Authorized*
Argentina	Estrictamente Secreto	Secreto	Confidencial	Reservado
Australia	Top Secret	Secret	Confidential	Restricted
Austria	Streng Geheim	Geheim	Verschluss	
Belgium (Flemish)	Zeer Geheim	Geheim	Vertrouwelijk	Bepertke Verspreiding

*****Provided that this level of protection is at least equivalent to that provided by the foreign government, but less than U.S. Confidential.

Source: DOE M 470.4-4A.

Unclassified Matter Used to Simulate or Demonstrate Classified Matter for Training purposes

The following is taken from DOE M 470.4-4 chg 1 (archived).

Unclassified matter used to simulate or demonstrate classified matter for training purposes must be clearly marked to indicate it is unclassified. Examples of recommended training markings are as follows: "Training (Exhibit) Purposes Only," "Classified for Training Only," "Unclassified Sample," "Example (Exhibit) Only," or "S (C) for Training Only." These markings should be in large print and should be placed so it is clear the marking information is not classified.

Classified Page Changes that Result from Periodic Updates to a Classified Document

The following is taken from DOE M 470.4-4 chg 1 (archived).

Classified page changes:

- Periodic updates or revisions to a classified document may be transmitted as page changes instead of retransmitting the entire document. Individual page changes cannot be transmitted when the overall classification of the document has changed.
- The transmitting receipt for a page change should provide direction for incorporating the pages into the document.
  - If the classified document is not accountable, the new pages may be inserted and the obsolete pages destroyed properly.
  - If the classified document is accountable, the new pages may be inserted and the destruction of the obsolete pages documented according to local procedures. Although the page changes themselves do not need to be given unique identification numbers, a record of the page changes must be kept.

- Page changes must be marked in the same manner as the original document. For example, if the original document was portion-marked, the page change must be portion-marked, and if the category was marked on each page of the original document, it also must be marked on each page that is changed. Note: Also refer to DOE M 470.4-4 chg 1, (archived), paragraph 3.h.(2) which contains requirements for marking page changes.

File Folders and Other Containers Containing Classified Matter

The following is taken from DOE M 470.4-4 chg 1 (archived).

When not in approved secure storage containers, file folders, and other items containing classified matter must be marked conspicuously to indicate the highest classified level of any classified matter contained within.

- The classification level marking must be marked top and bottom on the front and back of the folder. The classification level marking is necessary only when the folder containing classified matter is removed from an approved security storage repository.
- Containers of classified documents such as videotapes, cassettes, and ESM also must include classification level markings on the top and bottom of the front and back of the container. However, if the subject container is too small to contain typical classification levels on top and bottom, a single label may be placed in the middle of the case. When marked with the classification level, these containers act as cover sheets to alert observers about appropriate protection and handling requirements. If these containers are used for shipping, consider them an inner envelope only and address and mark them appropriately. Note: The plastic encasing the actual tape, cassette, or ESM is not considered a container for the purposes of these marking instructions. Only the removable covering of a cassette, tape, or ESM is considered a container.

Working Papers

The following is taken from DOE M 470.4-4 chg 1 (archived).

Classified working papers and drafts are considered to be interim production stages toward the generation of a permanent document. Hard copies of working papers and drafts must contain the following markings:

- The date created.
- The highest potential overall classification level of the draft or working paper at the top and bottom of the outside of the cover page (if any), on the title page (if any), on the first page of text, and on the outside of the back cover or last page. Each interior page of a classified document must be marked at the top and bottom with the highest classification of that page (including unclassified), or the overall classification of the document.
- The overall category (if RD or FRD) of the draft or working paper must be marked on the cover page (if any), title page (if any), or the first page of text. The category

marking is not required on draft and working paper interior pages that contain RD or FRD information.
- The annotation "Working Paper" or "Draft" must be marked on the first page of text.
- Any applicable caveats or special markings must be annotated on the cover page (if any), title page (if any), or the first page of text.

Electronic and facsimile versions of working papers and drafts are marked as required by DOE M 470.4-4 chg 1 (archived), paragraph 3p(3) and (4). Classified working papers and drafts may be transmitted within work groups without being marked as final documents. Work groups may consist of individuals from multiple organizations (see DOE M 470.4-4 chg 1 (archived), paragraph 3.p.(3)(b)4.a.).

Markings prescribed for a finished document must be applied when a draft or working paper meets the following requirements:
- Released by the originator outside the activity or office
- Retained for more than one hundred-eighty days from the date of origin
- Filed permanently

Classified documents that are updated on a frequent basis, commonly referred to as "living documents" (e.g., documents that are part of an ongoing experiment or study) may be considered as originating each date they are changed.
- Local procedures must provide a specific technique to demonstrate that the "living document" is in fact being changed frequently (e.g., a sheet attached to the front of the document that gives the number of pages and the date of the last change is an example of such a technique).
- Each version of a "living document" that has been superseded by an updated version, retains its initially assigned origination date for the purpose of determining requirements for marking it as a finished document.

35. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for the management of the marking of classified documents received from OGA and foreign governments not conforming to DOE requirements.

a. Discuss the procedure for the proper marking of documents received from OGA and/or foreign governments.

The following is taken from DOE M 470.4-4A.

As a rule, documents received from OGAs and foreign governments that have not been marked to conform to DOE requirements do not need to be re-marked. However, all documents received must clearly indicate a classification level and category (if RD or FRD). The sender must be contacted to resolve any marking questions.

36. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for control and accountability systems used to prevent unauthorized access to or removal of classified information.

a. List the different types of accountable matter.

The following is taken from DOE M 470.4-4A.

The following are types of accountable matter:

- TS matter.
- S matter stored outside an LA (or higher).
- Any matter that requires accountability because of national, international, or programmatic requirements such as the following:
  - Classified computer equipment and media supporting the Nuclear Emergency Support Team and Accident Response Group operations and similar elements.
  - National requirements such as cryptography and designated communications security.
  - International requirements such as NATO "Restricted Data" or "Formerly Restricted Data" (ATOMAL), designated U.K. documents, or other FGI designated in international agreements.
  - Designated SAPs.
  - Sigma 14.
- Classified Removable Electronic Media (CREM), which is required to be marked as S/RD or higher classification, or which is otherwise accountable (DOE M 470.4-4A, paragraphs 5.b.(2) and (3)). Each piece of ACREM must remain in accountability until verification that none of the information that requires the CREM to be accountable can be retrieved or recovered from that piece of CREM. Only National Security Agency-approved methods or other officially approved methods that comply with DOE CS policy may be used to determine whether information is recoverable from ACREM. Any such approved methods or criteria must be performance-tested as necessary to ensure that unauthorized access to classified information does not occur.

b. Discuss the policies and procedures for the accounting of Classified Removable Electronic Media (CREM).

The following is taken from DOE M 470.4-4A.

At least one appointed and trained ACREM custodian and alternate ACREM custodian must be assigned for each secure storage repository or file cabinet used to store ACREM. If more than one custodian and one alternate custodian are assigned, the number of individuals assigned to these positions must be identified and justified through documented CSA-approved procedures and must be kept to the minimum number necessary, based on operational need and associated risk.

These appointed individuals are responsible and accountable for ACREM, all accountability records, and other duties outlined in CSA-approved local procedures that must include, but are not limited to: a documented ACREM check-out and transfer process implemented to record all ACREM transfers between ACREM custodians, alternate ACREM custodians, and users. This process must be performance-tested to ensure its effectiveness.

c. Discuss the policies and procedures for the use of control stations to maintain records and access lists.

The following is taken from DOE M 470.4-4A.

Control stations must be established to maintain records, accountability systems, access lists (when required), and control classified matter (including facsimiles) received by and/or dispatched from facilities. Control station operators must maintain accountability systems for accountable matter. A defined and operated ACREM accountability process may function as a control station.

d. Discuss the development and maintenance of accountability systems and records.

The following is taken from DOE M 470.4-4A.

Accountability records are required when accountable matter is originated, reproduced, transmitted, received, destroyed, permanently buried, or changed in classification. All sites must develop procedures to ensure that all accountable matter has been entered into accountability systems. At a minimum, accountability records must indicate the following information for each item of accountable matter. If accountable matter is received from another agency and lacks a unique identification number, one must be assigned.

- Date of the Matter. The date the matter was originated or created. For documents, this term means the date the document was finalized.
- Brief Description of the Matter (unclassified, if possible). Examples include the unclassified title (if a document) or description (if material). It may also be helpful to describe the form of the matter (e.g., a document, magnetic medium, microform, drawing, photograph, or photographic negative). If a title or description is classified, an unclassified descriptor should be used to prevent the accountability records system from becoming classified.
- Unique Identification Number. This could be a unique document number (if a document) or serial number (if material). Unique identification numbers may be provided by creating a totally new number for each individual document, including copies, or by adding the copy and series to the old base number when reproducing accountable documents. The key point is to ensure that each document, whether an original or a reproduction, has a unique number associated with it.
- Classification Level (and Category, if RD or FRD) and Caveats. Classification level, category (if RD or FRD), and additional handling caveats, if any, of the matter must also be indicated.

- Number of Copies and Disposition. The number of copies of a document (including the original) generated during either origination or reproduction, the disposition of each copy (e.g., destruction, downgrading, declassification, dispatch outside the facility, or incorporation into another accountability record), and the date of disposition. The term "disposition" varies in meaning as follows regarding
  - origination, transmission, receipt, and reproduction, "disposition" means the offices or activities where the matter was distributed;
  - destruction, "disposition" means the organization where the matter was destroyed and by whom; or
  - change of classification, "disposition" means which office or activity performed the change of classification and which offices or activities have copies of the matter.
- Originator Identification. The organization name and address of the originator. For material, this information is found in the associated paperwork.
- Authority for Contractor Retention. Contract or other written retention authority that authorizes the matter to be in the possession of a contractor. This authorization can be either a letter of authorization or a contract reference to the authorization to retain classified matter. A copy of this authorization should be maintained with the accountability records and should be readily available to facilitate compliance disposition reviews.
- Date Received (if applicable). The date the transmitted matter arrived.
- Activity from Which the Matter was Received (if applicable). The office or activity name and address from which matter was transmitted to the recipient.
- Responsible Individual. The individual who checked it in and/or out (who has personal responsibility for it).

e. Discuss the policies and procedures for maintaining an inventory of accountable documents and matter.

The following is taken from DOE M 470.4-4A.

All ACREM must be inventoried and all results documented on a recurrent basis. All discrepancies between ACREM records and the verified locations and status of all ACREM, must be identified and reconciled (examples of status include possessed by an identified individual, stored, or destroyed).

- The current and previous individual assigned control/possession of all ACREM, according to their assigned custodians and users, must be documented and available at any given time within retention periods.
- The baseline required frequency of the recurrent ACREM inventories is monthly. However, the DOE CSA may increase the time between inventories up to a maximum of six months.
- Inventories are not required for ACREM maintained in a locked file cabinet or GSA approved security container that is located in a vault or CA, or is maintained in security containers with XO-series locks, and the container has not been accessed

since the last inventory. However, time between inventories must not exceed one year (three hundred sixty-five calendar days) for any ACREM.

f. Discuss the policies and procedures for the maintenance of records, master files and databases, and working papers and drafts.

The following is taken from DOE M 470.4-4 chg 1 (archived).

Records

Records maintained to control and account for classified matter, including those reflecting receipt, dispatch, and destruction, must be retained in accordance with the DOE records schedule and the NARA's GRS 18.

Master Files and Databases

Master files and databases created in central data processing facilities to supplement or replace TS records are not authorized for disposal under this GRS. These files must be scheduled on an SF 115, *Request for Records Disposition Authority*.

Working Papers and Drafts

Classified working papers and drafts are considered to be interim production stages toward the generation of a permanent document. Working papers and drafts must be

- protected in accordance with the assigned classification;
- destroyed when no longer needed; and
- accounted for and controlled in the manner prescribed for a finished document when the working papers and drafts meet the following requirements:
  - released by the originator outside the originating activity or work group (a work group may consist of individuals from multiple organizations that is established to support the activity);
  - retained for more than one hundred eighty days from the date of origin; or
  - filed permanently.

g. Discuss the requirements governing the establishment and use of automated accountability systems and electronic receipting.

The following is taken from DOE M 470.4-4A.

Automated accountability systems must

- be approved by the DOE CSA;
- implement the requirements under DOE M 470.4-4A, paragraph 5.e.; and
- provide security controls to ensure that no unauthorized changes are made to system records.

Electronic receipting systems are approved as long as the following conditions are met. The system

- is approved by the DOE CSA;

- provides identification of both the individual and the document disposition; and
- provides adequate security controls to ensure that no unauthorized changes are made to the system record.

37. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for the reproduction of classified information.

a. Discuss the general regulations for reproducing classified documents.

The following is taken from DOE M 470.4-4A.

CSA-approved procedures must be established for the reproduction of classified matter. Reproduction of classified matter must be limited to the minimum number of copies consistent with operational requirements and any other pertinent reproduction limitations.

Local procedures should address the issue of controlling the number of copies of classified documents.

Reproduction must be accomplished by authorized persons who know the procedures for classified reproduction and only in the performance of official or contractual duties.

Classified documents may be reproduced without originator approval except when they contain markings that limit reproduction.

To restrict reproduction of a classified document, consider one of the following techniques:
- For intelligence documents only, the originator controlled caveat marking may be used to restrict reproduction to that allowed by the originator.
- Originators of non-intelligence documents who wish to prevent unlimited copying of a classified document may use the markings restricting duplication without originator approval.

When any of the data that reside on a piece of ACREM (source media, in this case) is moved to, or reproduced on, another piece of media, the receiving media immediately becomes (or remains) accountable because it must be assumed to contain that which made the source media accountable, until proven otherwise and approved by the DOE CSA.

b. Discuss the policies and procedures concerning the use of equipment used to reproduce classified information.

The following is taken from DOE M 470.4-4A.

Classified matter must be reproduced on equipment specifically approved and designated for this purpose to ensure minimal risk of unauthorized disclosure or access. To the greatest extent possible, this equipment must be located within LAs, PAs, EAs, or MAAs.

- Classified copying must not be performed in the presence of individuals lacking the proper security clearances or need-to-know.
- Ensure all machines to be used for reproducing classified documents are approved in accordance with local procedures and CS policy.

c. Discuss the procedures for reproducing documents received from outside agencies.

The following is taken from DOE M 470.4-4A.

Outside agency documents may be reproduced in accordance with the same rules and restrictions that exist for DOE documents. Therefore, unless specific instructions to the contrary accompany the documents, they may be reproduced. For example, National Security Council (NSC) documents will have a copy restriction notice; therefore, NSC documents will be reproduced only with the permission of the originator.

d. Discuss the requirements for reproduction of CREM.

The following is taken from DOE M 470.4-4A.

When any of the data that reside on a piece of ACREM (source media, in this case) is moved to, or reproduced on, another piece of media, the receiving media immediately becomes (or remains) accountable because it must be assumed to contain that which made the source media accountable, until proven otherwise and approved by the DOE CSA.

38. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for receiving and transmitting classified matter.

a. Discuss the general rules for the transmission and receipt of classified matter.

The following is taken from DOE M 470.4-4A.

Classified matter must be transmitted only in the performance of official or contractual duties. If the transmission is not required by the specific terms of the contract or required for performance of the contract, contractors must obtain written authorization from the DOE CSA before transmitting classified matter outside the facility. Before transmitting classified matter, the sender must ensure

- the recipient has the appropriate security clearance, has any required programmatic or special access approval, and meets the need-to-know criteria.
- an approved classified address has been identified and used for the appropriate method of transmission, (e.g., mailing, shipping, or overnight delivery).

b. Discuss the controls that must be applied to classified matter received at a facility.

The following is taken from DOE M 470.4-4A.

When classified matter is received at a facility, the following controls must apply:

- Classified matter must be delivered to personnel designated to receive it at a control station with the inner envelope unopened. Procedures must be established to ensure that when classified matter is not received directly by the designated control station (regardless of the type of mail system), the inner container remains unopened.
- The package must be examined for evidence of tampering and the classified contents checked against the receipt (if provided). Evidence of tampering must be maintained and reported promptly to the CSA. If the matter was received through the U.S. Postal Service, the appropriate U.S. Postal Inspector must also be notified promptly. Discrepancies in the contents of a package must be reported immediately to the sender. If the package (or container) is in order and includes a receipt, the receipt must be signed and returned to the sender.

c. Discuss the methods for packaging classified matter that is to be transmitted outside or inside a facility.

The following is taken from DOE M 470.4-4A.

Classified matter to be transmitted outside a facility must be double-wrapped (enclosed in opaque inner and outer containers) except as specified below. The contents of the package or shipment must be securely packaged to meet DOE and the applicable transporting agency's requirements, (e.g., the U.S. Postal Service) for transmission.

- Envelopes and Similar Wrappers. All classified information physically transmitted outside facilities must be enclosed in two layers, both of which provide appropriate protection and reasonable evidence of tampering and which conceal the contents. The inner enclosure must clearly identify the classified address of the sender and the intended recipient, the highest overall classification level, and category (if RD or FRD), of the contents, and any appropriate warning notices. The outer enclosure must be the same except that no markings to indicate that the contents are classified must be visible. Intended recipients must be identified by name only as part of an attention line.
- Other Containers. The outer container must maintain the integrity of the inner container.

d. Discuss the use and contents of form DOE F 5635.3, Classified Document Receipt.

The following is taken from DOE M 470.4-4A.

When transmitting S or C classified matter outside site/facilities by any method, a receipt must be used. Receipts must identify the classified contents and the names and addresses of both the sending and receiving facilities. Receipts must not contain classified information. If

not practical, the receipt may be sent to the recipient with the required advance notification of shipment or may be hand-carried. When classified matter is transmitted by courier, DOE F 5635.3, or a receipt comparable in content must be used.

The receipt must be prepared in triplicate and remain unclassified when completed. Two copies of the receipt must be placed in the inner container with the matter (except as noted above) and sent to the intended recipient. The third copy must be maintained by the sender until the original is signed and returned. The receipt must contain the following information:

- Full names of the sender and the recipient
- Unclassified address of the sender, unless the receipt contains classified information and a classified mailing address for the sender is required
- Classified address of the recipient
- Description of the classified matter (e.g., title or other means)
- Date of the matter
- Classification of the matter
- Unique identification number, if accountable

A separate receipt must be completed for each recipient regardless of the number of items for each recipient.

e. Discuss the policies and procedures for using classified addresses.

The following is taken from DOE M 470.4-4A.

Classified addresses must be verified through the SSIMS or the Defense Security Service (DSS). If not in either system, a new classified mail channel must be established. See DOE M 470.4-1 chg 1 for additional requirements.

Hard-copy printouts of the SSIMS or DSS classified addresses can only be used to validate approved classified addresses for thirty calendar days from print date.

f. Discuss the policies and procedures for hand-carrying classified matter outside of a facility.

The following is taken from DOE M 470.4-4A.

The following requirements apply to hand-carrying classified matter; however, the requirements identified in DOE M 470.4-4A, paragraph 7.1, also apply to hand-carrying bulk documents.

- Local procedures must be developed describing the process for obtaining approval (including approval authority) to hand-carry outside of a site/facility and for providing notification when removing classified matter from the facility. Local hand-carry procedures must be approved by the CSA.

- A record/receipt of the classified matter must be made before departure, retained by the employee, and inventory must be made of the matter for which the employee was charged. The record should contain the following information:
  - Subject or title (unclassified, if possible)
  - Date the matter was removed from the facility
  - Signature of the person removing the matter
  - Date the matter was returned; or date and recipient's name and organization from receipt for matter that was transferred to another individual
- The removal of classified matter from approved facilities to private residences or other unapproved places (e.g., hotel or motel rooms) is prohibited.
- Contingency plans for delayed arrival must cover alternative protection and storage procedures, reporting requirements, and be approved by the CSA.
- Classified matter may be hand-carried outside the U.S., provided the following conditions are met:
  - The traveler must possess appropriate security clearance and a diplomatic passport. Diplomatic passports can only be issued to Federal personnel attached to a mission or embassy as a tenant or performing a mission under the auspices of the Department of State.
  - The traveler must obtain written authorization from the cognizant departmental element.
- Requirements for security screening of classified matter at airports are established by the Transportation Security Administration.

g. Discuss the policies and procedures for use of commercial express service organizations for transmitting classified matter outside of a facility.

The following is taken from DOE M 470.4-4A.

The use of commercial express service organizations for transmitting classified matter is restricted to emergency situations and the matter must be delivered to and secured at the receiving location the next calendar day.

At a minimum, the sender must ensure that the following conditions are met:
- The use of the express service organization has been approved by the sender's DOE CSA and an address for receiving deliveries from the express service has been input into SSIMS for the receiving organization.
- The address selected for the overnight/commercial express service cannot be greater than five lines, cannot be a post office box, and must be a street address.
- The intended recipients must be notified twenty-four hours in advance (or immediately if transit time is less than twenty-four hours) of the proposed shipment and arrival dates.
- All packages are double-wrapped before being inserted into the packaging provided by the commercial express service organization.

- In accordance with packaging requirements, commercial express service packages must not be identified as classified packages.
- The properly wrapped packages are hand-carried to the express mail dispatch center or picked up from a control station in sufficient time to allow for dispatch on the same day.
- Commercial express carrier drop boxes must not be used for classified packages.
- Facilities should include specific details regarding the use of package tracking in local procedures. The commercial express carrier may be contacted for details regarding packaging requirements.

Problems with the delivery of classified matter via commercial express service delivery must be reported according to the reporting of security incidents (see DOE M 470.4-1 chg 1).

39. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for the disposition of classified matter in the event of a contract closeout or a FCL termination.

a. Discuss the reporting requirements for the disposition of classified matter upon contract completion.

The following is taken from DOE M 470.4-4 chg 1 (archived).

Classified matter received or generated in the performance of a classified contract must be returned to DOE on completion of the contract unless the matter has been declassified or destroyed or retention is authorized. DOE M 470.4-1 chg 1 and DOE 470.4-4 chg 1, section A, require that line management implement the procedures developed by the cognizant DOE line management in coordination with the DOE CSA for contract closeout and facility termination.

When a contract is completed, the contractor usually destroys or returns all classified matter unless it provides a benefit to DOE for the contractor to retain the classified matter. Upon completion or termination of a contract, the contractor must submit to the contracting officer either a certificate of non-possession or a certificate of possession (of classified matter). The contracting officer must then transmit the certificate to the DOE CSA.

Upon return or destruction of all classified matter pertaining to a contract, the contractor must submit a certificate of non-possession to the CSA. The certificate must include the contract number and a statement that all classified matter has been returned or destroyed.

b. Discuss the policies and procedures for disposition of classified matter in the termination of a FCL.

The following is taken from DOE 470.4-4 chg 1 (archived).

If an FCL is terminated for any reason, classified matter in the facility's possession must be returned to DOE or disposed of according to instructions from the CSA. A certificate of non-possession must be completed as part of the clearance termination process. For prime contracts, DOE is the CSA. To accomplish the termination requirements, the CSA must ensure the following steps are accomplished.

- Determine whether a moratorium or ongoing litigation restricts actions.
- Acquire all classified matter not authorized for destruction.
- Conduct a 100 percent inventory of all accountable matter, taking appropriate action if any matter is missing.
- Check to ensure that all matter has been returned, if applicable.
- Destroy all copies, except record copies, of all classified documents.
- Send all remaining classified matter to the site specified by the responsible contracting officer and CSA.

Once the matter is destroyed or transferred, the CSA must complete the facility termination procedures (see DOE M 470.4-1 chg 1).

40. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for the destruction of classified matter.

a. Discuss the identification of classified matter subject to destruction.

The following is taken from DOE M 470.4-4A.

Classified matter that is generated, received, transmitted, used, stored, reproduced, permanently placed (buried according to the requirements of DOE M 470.4-4A), or destroyed must be protected and controlled commensurate with classification level, category (if RD/FRD), and caveats (if applicable). All pertinent attributes must be used to determine the degree of protection and control required to prevent unauthorized access to classified matter.

Accountability records are required when accountable matter is originated, reproduced, transmitted, received, destroyed, permanently buried, or changed in classification. This could require a unique identification number (if a document) or serial number (if material). Unique identification numbers may be provided by creating a totally new number for each individual document, including copies, or by adding the copy and series to the old base number when reproducing accountable documents. The key point is to ensure that each document, whether an original or a reproduction, has a unique number associated with it.

Destruction of accountable classified matter must be documented on DOE F 5635.9, *Record of Destruction*, or a form similar in content, which must be signed by both the individual destroying the matter and the witness.

b. Discuss the procedures to be followed in the destruction of classified matter under a court order prohibiting destruction.

The following is taken from DOE M 470.4-4A.

If under a court order prohibiting destruction, special destruction procedures may be required. Under such circumstances, all destruction activities must be conducted in accordance with guidance provided by the DOE Office of General Counsel and the appropriate records management organization.

c. Discuss the authorized types of destruction and the special requirements that must be satisfied when classified matter is destroyed.

The following is taken from DOE M 470.4-4A.

Classified matter must be destroyed beyond recognition to preclude subsequent access to any classified information. ESM must be destroyed according to the DOE CS directives. Destruction techniques include burning, shredding, pulping, melting, mutilating, pulverizing, or chemical decomposition. The following additional requirements must be satisfied when classified matter is destroyed:

- The DOE CSA must approve the use of public destruction facilities and any other alternative procedures.
- If classified matter cannot be destroyed onsite, it may be destroyed at a public destruction facility. If a public destruction facility is used, an appropriately cleared individual must ensure the destruction occurs on the same day it leaves a cleared facility and that the destruction is properly witnessed. A record of dispatch is required when the matter is released to another cleared contractor or OGA.
- Ash residue produced by burning must be examined and reduced by physical disturbance to ensure that the matter is completely destroyed and no ash residue matter remains to prevent the release of classified information or subsequent analysis.
- Classified microforms must be destroyed by burning, chemical decomposition, disintegration, or other methods approved by the CSA.
- Classified ESM destruction must include examination to ensure that the media is no longer usable and that no classified information is present or recoverable. Classified ESM destruction must be completed according to the DOE CS requirements.

d. Discuss the policies and procedures for the destruction of classified matter by the use of approved equipment.

The following is taken from DOE M 470.4-4A.

Classified matter must be destroyed by equipment that has been approved by the CSA and according to specific manufacturer's instructions. The residue output must be inspected each time destruction is effected to ensure that established requirements have been met.

Shredders:

- Crosscut shredders used for the destruction of classified paper matter and non-paper products, excluding microfilm, must produce residue with a particle size not exceeding 1 mm in width by 5 mm in length.
- Crosscut shredders purchased prior to December 31, 2003, that produce residue with particle sizes not exceeding 1/32 of an inch in width by ½ inch in length may continue to be used for the destruction of classified paper matter and non-paper products, excluding microfilm. However, these shredders must not be used once they cannot be repaired or restored to cut residue within the 1/32-inch width by ½-inch maximum particle dimensions.

Pulping equipment must be equipped with security screens with perforations of ¼ inch or smaller.

Pulverizing equipment must be outfitted with security screens that meet the following specifications:

- Hammer mill perforations must not exceed 3/16 inch in diameter.
- Chopper and hybridized disintegrator perforations must not exceed 3/32 inch in diameter.

e. Discuss the requirements for witnesses during the destruction of classified matter.

The following is taken from DOE M 470.4-4A.

The destruction of classified matter must be ensured by an individual(s) who has/have appropriate security clearance for the classification level, category (if RD or FRD), and any applicable caveats of the matter to be destroyed. The destruction of non-accountable classified matter may be accomplished by one individual; no witness is required. The destruction of accountable matter must be witnessed by an appropriately cleared individual other than the person destroying the matter.

f. Discuss the requirements for creation and retention of records of destruction when classified matter is destroyed.

The following is taken from DOE M 470.4-4A.

Accountable matter—Destruction of accountable classified matter must be documented on DOE F 5635.9 or a form similar in content, which must be signed by both the individual destroying the matter and the witness.

Non-accountable matter does not require destruction receipts or certificates.

g. Discuss the policies and procedures for the disposition of classified waste.

The following is taken from DOE M 470.4-4 chg 1 (archived).

Classified waste must be destroyed by approved methods as soon as practical. Receptacles used to accumulate classified waste must be clearly marked to indicate their purpose. Pending destruction, classified waste and receptacles must be protected as required for the level and category of classified matter involved.

- Non-accountable classified matter (i.e., any matter classified as S or C that is not entered into an accountability system) may be destroyed as classified scrap or waste.
- Regardless of the method selected to store classified scrap pending destruction, certain considerations should be taken into account:
  - Accountable matter should never be placed in containers (e.g., envelopes, files, and security container drawers) used as repositories for classified scrap.
  - Containers should be emptied frequently enough to ensure that classified matter is destroyed within one hundred eighty days of origination.

41. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for managing foreign government information.

a. Discuss the policies and procedures for safeguarding classified matter furnished by foreign governments and U.S. information that may be combined with it.

The following is taken from DOE M 470.4-4A.

Foreign government information must be safeguarded to provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When equivalent, standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. C information, including allowing access to individuals with a need to know who have not otherwise been cleared for access to classified information.

To ensure the protection of classified FGI according to EO 12958, *Classified National Security Information*, as amended, the following requirements must be met:

- Handling. Classified documents received from foreign governments do not require portion marking. Such documents generated and marked entirely by a foreign government must be protected commensurate with the classification level the foreign government specified.
- Marking.
  - A derivative classifier or classification officer must be contacted with any questions regarding the appropriate classification level for a foreign government information document.
  - Documents generated by a foreign government in which U.S. information has been added must be reviewed for classification by a derivative classifier or classification officer, marked, and protected accordingly.

- If the original markings in the foreign government documents are readily recognizable as related to a U.S. classification requiring special protection and control, the documents do not require re-marking.
- If the foreign government marking is not readily recognizable as related to a U.S. classification, the foreign government document must be reviewed by a derivative classifier or classification officer, and an equivalent U.S. classification must be applied.
- If the fact that the information is FGI must be concealed, the document must be marked as if it were wholly of U.S. origin.

Further information on protection of FGI can be found in DOE M 470.4-4A, section A.

42. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for the marking and accountability of classified material.

a. Discuss the policies and procedures for marking classified material.

The following is taken from DOE M 470.4-4A.

All classified matter, regardless of level and category, must be marked to ensure information is appropriately protected to prevent inadvertent disclosure. Classified matter must be reviewed and brought up to current marking standards whenever it is released by the current holder ("current holder" may be defined as an individual, specific office, or AHWG) or removed from archival storage.

Classified matter, regardless of date or agency of origin must be marked to indicate at least the classification level and category.

- Classified NSI documents that were created after April 1, 1996, and that lack appropriate current markings including declassification on a date or event, classification basis, or classifier's name, must be reviewed by a derivative classifier to ensure the classification level and category are still correct and then re-marked to bring them up to current marking requirements.
- Classified matter retained for litigation or for official archival purposes, including classified matter transferred during site closure, need not be brought up to current marking standards.
- DOE M 475.1-1B provides requirements for reviewing and marking documents with obsolete markings.

All classification markings must be distinguishable from the document text. The overall classification level (i.e., TS, S, or C) of a document must be marked on the top and bottom of the cover page (if any), the title page (if any), the first page of text, and the outside of the back cover or last page of text. The classification level and category (if RD or FRD) must be clearly marked on all other (non-document) classified matter if possible. Otherwise, alternative marking methods must be used to identify the overall classification level and

category (if RD or FRD). When marking the level or category is not practical, written notification must be furnished to all recipients. The originator is responsible for ensuring that classified matter is marked according to DOE M 470.4-4A. DOE M 475.1-1B contains additional marking requirements beyond the requirements contained in DOE M 470.4-4A.

All interior pages of documents must be marked top and bottom with either: the overall classification level and category (if RD or FRD) for the entire document, or the highest classification level and category (if RD or FRD) of all information on that page; or with the appropriate unclassified marking if there is no classified information on that page.

b. Discuss the accountability requirements for classified material.

The following is taken from DOE M 470.4-4A.

The material accountability system must provide a description of each type of item, the classification level and category (if RD or FRD), the number of items of each type, and scheduled inventories. Part numbers and serial numbers should be used, when available, either to assist with unique numbers or identify types of material. Where applicable, the production cycle and production control procedures can be used to facilitate the conduct of all inventories of accountable material. Accountability procedures must be approved by the CSA.

Exemptions—when they are not applicable, the following items are exempt from inclusion in the material accountability records:

- Matter date
- Number of copies
- Date and disposition of reproduction

43. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for OPSEC.

a. Discuss the required activities that must be included in an OPSEC program.

The following is taken from DOE M 470.4-4A.

An OPSEC program(s) must be implemented covering each program office, site, and facility to ensure the protection of Critical Program Information (CPI) and to assist in ensuring the protection of classified matter. The OPSEC program, in addition to ensuring the compliance with the requirements of DOE M 470.4-4A, must also include the following activities:

- Establish a point of contact with overall OPSEC responsibilities for each site, facility, and program office whose name and contact information will be provided to the Office of Health, Safety and Security.
- Ensure OPSEC point of contact participation in the development of local implementation training and/or briefings tailored to the job duties of the individual employees.

- Develop and execute comprehensive OPSEC awareness program that includes regular briefings to ensure that personnel are aware of their responsibilities in support of the OPSEC program.
- Participate in self-assessments to ensure the requirements to protect and control classified matter and CPI are being followed in all areas and that employees are aware of their responsibilities.
- Provide information concerning deviations involving the OPSEC program to the Office of Health, Safety and Security and to the Associate Administrator for Defense Nuclear Security when involving NNSA facilities, in a timely fashion, to include implementation and expiration of such actions.
- Promulgate new OPSEC requirements to all affected employees.
- Interact and coordinate with Office of Health, Safety and Security on OPSEC national and departmental requirements interpretation and local implementation activities.

b. Discuss the planning, reviewing, and updating requirements for the OPSEC program.

The following is taken from DOE M 470.4-4A.

OPSEC plans must be developed for programs and operations and approved by the CSA. OPSEC plans must be reviewed and updated annually (at least every twelve months).

c. Discuss the identification and maintenance of Critical Program Information (CPI), including a discussion of indicators of CPI.

The following is taken from DOE M 470.4-4A.

Critical Program Information must be identified, including operational and programmatic data that would have a negative impact on national security and/or departmental operations if unauthorized disclosure should occur. The CPI must be

- prioritized according to the level of impact posed by an unauthorized disclosure. The CPI may be supported by a list of indicators that, when aggregated and analyzed, inappropriately reveal elements of the CPI.
- reviewed on a continuing basis. Results of the CPI reviews must be documented and maintained in program files.

d. Discuss the policies and procedures for conducting and reporting the results of OPSEC assessments.

The following is taken from DOE M 470.4-4A.

OPSEC assessments must be conducted at facilities having category I SNM (or credible roll-up of category II to a category I quantity), TS or SAP information within their boundaries. OPSEC assessments must be conducted at other facilities involved in creating, handling, storing, processing, transmitting, or destroying CPI as deemed necessary by the CSA.

- Either the programmatic or facility approach may be used to conduct OPSEC assessments. If the facility approach is used, all activities at the facility must be included in the assessment. If the programmatic approach is used, all activities within the program must be included in the assessment.
- When using the programmatic approach, the assessment team must ensure that CPI pertaining to category I SNM (or credible roll-up of category II to a category I quantity), TS matter or SAPs are assessed. Schedule and priority for conducting assessments will be based on CPI, threat assessments, risk management principles, recommendations received from the local OPSEC program, and direction from DOE line management.

e. Discuss the policies and procedures for conducting and reporting the results of OPSEC reviews.

The following is taken from DOE M 470.4-4A.

OPSEC reviews must be conducted to identify changing priorities in the local OPSEC program. OPSEC reviews are limited information-gathering activities to provide the data necessary to schedule and implement OPSEC actions. Results of OPSEC reviews must be documented.

- OPSEC reviews of sensitive activities and facilities must be conducted whenever the following criteria are met:
  - New construction is planned for a facility that will process or store classified or sensitive information or matter.
  - New sensitive activities are initiated or existing programs incur significant changes.
  - A sensitive program or activity has not been the subject of an OPSEC assessment or OPSEC review for the preceding two years.

f. Discuss the restrictions on information that will be posted to publicly available web sites.

The following is taken from DOE M 470.4-4A.

Information to be posted to publicly available websites:

- Before any information generated by or for the Federal government is placed on a DOE, DOE contractor, or sub-contractor or sub-contractor website or is otherwise made available to the public, it must be reviewed to ensure that it does not contain classified information or CPI. Before DOE contractors or subcontractors post government information to a personal or non-DOE website, it must be reviewed for the same concerns. The review process must include a multi-layer review to ensure suitability of the information for worldwide public release.
- Automated analysis tools should be used to assist in the review of information to determine if it is appropriate to release it to the public. Certain categories of

unclassified information are generally recognized as unsuitable for public release. Evaluation factors include:
  - Sensitivity. If the information is released to the public, it must not reveal or identify sensitive information, activities or programs.
  - Risk. Information that may be used by adversaries to the detriment of employees, the public, the department, or the nation must not be approved for release.
- Local procedures must be established for conducting information reviews and acquiring approval according to direction from the head of their respective departmental element. These procedures must identify specific information and information categories considered unsuitable for release to the public.

g. Discuss the vulnerabilities and countermeasures.

This subject is covered in DOE M 470.4-4A, section D, which is for Official Use Only.

44. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for SAPs.

a. Discuss the policies and procedures for SAPs authorized for use within the Department.

All SAPs must be approved by the Secretary or Deputy Secretary, based upon the recommendation of the SAP Oversight Committee (SAPOC), which manages and oversees the development of SAP security policies and procedures outline in DOE M 471.2-3B which is for Official Use Only.

The following is taken from DOE M 470.4-4A.

SAPs must be limited to acquisition, operations, support, and intelligence activities.

DOE and non-DOE (work for others) SAPs, with the exception of intelligence SAPs, must be registered manually (not in the SSIMS) through the established FCL process using DOE F 470.2, *Facility Data Approval Record (FDAR)* and DOE F 470.1, *Contract Security Classification Specification*, DoD F 254, or form similar in content. For additional information regarding FDAR process, see DOE M 470.4-1 chg 1. The FDAR and other forms must be classified according to classification guidance.

SAP facilities, work areas, and all activities must be surveyed according to DOE M 470.4-1 chg 1, by the cognizant SAP security coordinator in coordination with the cognizant program office and/or sponsor. Intelligence SAPs must be surveyed by the Office of Intelligence and Counterintelligence in conjunction with the sponsor. Independent oversight inspections must be performed for departmental programs according to DOE M 471.2-3B.

Protection program planning documents, including security plans and standard operating procedures, must comply with established SAP policies and program security manuals.

Any possible or probable loss, compromise, or unauthorized disclosure of SAP information must be reported to the appropriate government program manager, government program SO, DOE SAP security program manager (or cognizant SAP security coordinator), and the SAPOC's executive secretary according to established procedures. (DOE M 470.4-1 chg 1, section N, contains additional requirements.)

45. Safeguards and security personnel with the responsibility for IP must demonstrate a working level knowledge of the policies and procedures for protecting and controlling CUI.

a. Discuss the policies and procedures for protecting and controlling CUI.

The following is taken from the U.S. National Archives & Records Administration, *Controlled Unclassified Information Framework*.

The controlled unclassified information (CUI) framework refers to the policies and procedures governing the designation, marking, safeguarding, and dissemination of CUI terrorism-related information that originates in departments and agencies, regardless of the medium used for the display, storage or transmittal of such information.

Within the CUI framework, the 2008 Presidential Memorandum outlines what information can and cannot be designated as CUI. The CUI framework includes two levels of safeguards—controlled and controlled enhanced. It also includes two levels of dissemination—standard and specified.

Under the CUI framework, all CUI will be categorized into one of three combinations of safeguarding procedures and dissemination controls, which will be indicated through one of the three identified markings: 1) Controlled, 2) Standard; 3) Controlled, Specified; and Controlled Enhanced, Specified.

The CUI framework is a critical part of a larger effort to create an information sharing environment (ISE) that will facilitate the sharing of terrorism-related information. Because the CUI framework provides for standardized handling of information, it supports the individual missions of departments and agencies and enhances the ability to share vital terrorism-related information among Federal, state, local, tribal, private sector, and foreign partners. Implementing the CUI framework will advance the ISE and help departments and agencies better manage their information. The CUI office, with the advice of the CUI council, will develop and issue detailed CUI policy standards and implementation guidance for the CUI framework.

E. PERSONNEL SECURITY (PERS SEC)

Competencies and supporting knowledge and skills for section E, Personnel Security, are derived from the following DOE Orders, manuals, and guides:

- 10 CFR 710, "Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material"
- 10 CFR 712, "Human Reliability Program"
- DOE M 470.4-5, *Personnel Security*
- DOE O 470.4A, *Safeguards and Security Program*

46. Safeguards and security personnel with the responsibility for PERS SEC must demonstrate a working level knowledge of the access authorization (security clearance) process.

a. Discuss the following terms:

- **Derogatory information**
- **Access authorization**
- **Types of security clearances**
- **Types of access authorizations**
- **Types of background investigations**
- **Federal investigative standards**
- **Reciprocity**
- **Suspension**
- **Administrative Review (AR)**

Derogatory Information

The following is taken from 10 CFR 710.9.

If the reports of the investigation of an individual or other reliable information tend to establish the validity and significance of one or more items in the criteria, or of other reliable information or facts which are of security concern, although outside the scope of the stated categories, such information shall be regarded as derogatory and create a question as to the individual's access authorization eligibility.

Access Authorization

The following is taken from DOE M 470.4-7 (archived).

Access authorization means an administrative determination that an individual is eligible for access to classified matter or is eligible for access to, or control over, SNM.

Types of Security Clearances

The following is taken from DOE M 470.4-7 (archived).

Security clearances are administrative determinations that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted. The types of clearances are the same as those listed under types of access authorizations below.

Types of Access Authorizations

The following is taken from DOE M 470.4-5.

The type of access authorization requested is based on an individual's need for access to the category and level of classified information or matter, or category of SNM, for the performance of official duties. An authorization granted for access to SNM also allows access to the appropriate categories/levels of classified information or matter on a need-to-know basis.

There are five types of access authorization: Q, L, QX, LX, and QB. Determination of the type of access authorization must be certified in writing by the requester to the Director, Office of Headquarters Security Operations (for headquarters cases), or to the DOE CSA.

Types of Background Investigations

The following is taken from DOE M 470.4-5.

The following are the types of investigation most frequently conducted for the DOE:

- Single Scope Background Investigation (SSBI) is a full-field background investigation covering the most recent ten years of the individual's life.
- Single Scope Background Investigation-Periodic Reinvestigation (SSBI-PR) is a background investigation covering the most recent 5 years of the individual's life.
- National Agency Check with Law and Credit (NACLC) is a name check of the individual at appropriate Federal and local LEAs, a credit search, and a classification of the individual's fingerprints by the FBI.
- Access National Agency Check and Inquiries (ANACI) is a name check of the individual at appropriate Federal and local LEAs; a classification of the individual's fingerprints by the FBI; a credit search; and written inquiries regarding the individual's employment, education, residences, and references.
- Upgraded Investigation—the type of investigation requested may be upgraded to a more extensive investigation if the case appears to involve significant derogatory issues.
- Background Investigation by Other Federal Agencies—must be accepted in lieu of a new investigation provided that: the investigation meets the scope and extent of the required investigation; and the investigation was completed, or upgraded by reinvestigation, within the most recent five years.

Federal Investigative Standards

The following is taken from DOE M 470.4-5.

The investigative standard for a Q access authorization is an SSBI. The investigation for an L access authorization processed before October 1997 was a National Agency Check with Credit (NACC). For L access authorization requests initially processed after October 1997, the investigation is an NACLC for non-Federal employees and an ANACI for Federal employees.

Until March 1997, the Federal government did not have a defined investigative standard for reinvestigations, so each Federal agency established its own schedule and investigative standards for periodic reinvestigations. Therefore, if the previous security clearance or SCI approval is based on a reinvestigation, the DOE CSA must exercise judgment and latitude to determine if the investigation used by the other Federal agency is acceptable.

Reciprocity

The following is taken from DOE M 470.4-5.

Whenever possible, access authorizations are granted based on the interagency reciprocity procedures in DOE M 470.4-5, section H. Applicants for an access authorization will be processed according to these procedures if they have been cleared or are in the process of being cleared by another Federal agency.

Administrative Review (AR)

The following is taken from 10 CFR 710.20.

These procedures establish methods for the conduct of the AR of questions concerning an individual's eligibility for access authorization when it is determined that such questions cannot be favorably resolved by interview or other action.

b. Discuss the process for screening of investigation for "Q" and "L" access authorizations.

The following is taken from DOE M 470.4-5.

The investigative standard for a Q access authorization is an SSBI. The investigation for an L access authorization processed before October 1997 was an NACC. For L access authorization requests initially processed after October 1997, the investigation is an NACLC for non-Federal employees and an ANACI for Federal employees.

Until March 1997, the Federal government did not have a defined investigative standard for reinvestigations, so each Federal agency established its own schedule and investigative standards for periodic reinvestigations. Therefore, if the previous security clearance or SCI approval is based on a reinvestigation, the DOE CSA must exercise judgment and latitude to determine if the investigation used by the other Federal agency is acceptable.

c. Explain the purpose of the PERS SEC interview.

The following is taken from Standard Form 86, *Questionnaire for National Security Positions*.

Some investigations will include a personal interview with you as a normal part of the investigative process, providing the opportunity to update, clarify, and explain information on the form more completely, which often helps to complete the investigation faster.

47. Safeguards and security personnel with the responsibility for PERS SEC must demonstrate a working level knowledge of the policies, procedures, and governing requirements of the DOE PERS SEC program.

a. Describe the general requirements for determining the type of access authorization and investigative requirements, including those involving dual citizenship and foreign nationals.

The following is taken from DOE M 470.4-5.

General

When the duties of a position will require the incumbent to access DOE classified information or matter, or SNM, the contractor must process the selectee for either Q or L access authorization if the selectee does not already possess the appropriate type of access authorization. The type of access authorization to be requested will depend on the category (RD, FRD, or NSI) and level (TS, S, or C) of classified information or matter, or category of SNM (I, II, III, or IV) to which the incumbent will require access.

Where there are compelling reasons in furthering the DOE mission, foreign nationals (to include immigrant aliens) with a special expertise that is not possessed to a comparable degree by an available U.S. citizen may be granted access authorization only for specific programs, projects, contracts, licenses, certificates, or grants for which the individual needs access to classified information or matter, or SNM. Such individuals will not be eligible for access to any greater level of classified information than the U.S. government has determined may be releasable to the country of which the individual is currently a citizen, and such limited access may be approved only if the prior ten years of the individual's life can be appropriately investigated.

Dual Citizenship

Individuals who possess a dual citizenship (i.e., who are simultaneously a citizen of the U.S. and another country) and who have exercised citizenship rights in the foreign country, or have represented themselves as citizens of the foreign country, or who have intentions to do

so in the future, must meet the requirements for foreign nationals in DOE M 470.4-5, chapter VI, paragraphs 1 and 2. There are two alternatives to being processed as foreign nationals:

- If the individual is willing to renounce citizenship in the other country, the individual must provide a notarized statement attesting to the fact that the non-U.S. citizenship has been formally renounced, and if available, evidence that the renunciation has been formally accepted by an official representative of the other country's government.
- The DOE CSA, of the Director, Office of Security, for headquarters cases, may waive the requirement to renounce the non-U.S. citizenship if it is determined that it would be detrimental to the individual or to DOE security objectives, or that the risk associated with the individual maintaining the non-U.S. citizenship status has been adequately mitigated. A copy of the security evaluation documenting this waiver must be maintained in the individual's personal security file (PSF).

Foreign Nationals

For foreign nationals the DOE CSA must:

- Receive and consider requests for access authorizations for foreign nationals under their jurisdiction. Requests may be disapproved by the DOE CSA if the requirements of DOE M 470.4-5, chapter VI, paragraph1, have not been met.
- Interview the foreign national to determine steps taken by the individual to become a U.S. citizen; previous civilian or military service with a foreign government; family or other relatives abroad; family, legal, and financial ties abroad; and employment of relatives by a foreign government.
- Evaluate the risk arising from foreign national status, considering the following factors:
  - The nationality of the foreign national
  - Whether a sufficient security investigation can be conducted
  - Length of stay in the U.S.
  - Family, legal, and financial ties abroad
  - Whether and in what manner the foreign national has shown the intent to become a U.S. citizen
- Transmit the request to the Director, Office of Security, if it is determined that an adequate investigation can be conducted and the evaluation of risks described in DOE M 470.4-5, chapter VI, paragraph 2.a.(3) is favorable. The DOE CSA must include the following with the request:
  - A duplicate PSF, including the paperwork completed by the individual and a transcript of the interview
  - A statement concerning the program for which the foreign national has been recruited and the specific access to classified information or matter, or SNM, to be afforded
  - A statement that a favorable risk evaluation has been completed based upon the factors described in DOE M 470.4-5, chapter VI, paragraph 2.a.(3).

The Director, Office of Security must:

- Coordinate the following reviews/determinations:
  - The departmental element with programmatic authority for the relevant project must review the request for a foreign national's access authorization and determine whether the individual in question possesses special expertise necessary to a DOE program.
  - The review of the request for a foreign national access authorization to determine compliance with the requirements of the AEA concerning the release of RD to the government of the country where the foreign national holds citizenship.
- For foreign nationals, an SSBI is required for any type of access authorization.
- The determination to grant an access authorization to a foreign national can only be made by the DOE CSA or, in HQ, by the Director, Office of Security, without power of redelegation.
- An access authorization for a foreign national may only be extended, reinstated, or accepted for transfer with the concurrence of the departmental element having functional interest in the work to be done and after a new review as described in DOE M 470.4-5, chapter VI, paragraph 2.b.(1)(b).
- The Office of Security must maintain duplicate PSFs on all foreign nationals holding access authorizations. The processing personnel security office must provide copies of any additions to the PSFs on these individuals. Change of the individual's citizenship status must be reported to the Office of Security.

b. Describe the processes used for screening and analysis of PERS SEC cases and methods for determining access authorization eligibility.

The following is taken from DOE M 470.4-5.

Only DOE employees who are so authorized in writing may determine an individual's access authorization eligibility or render other formal determinations that affect an individual's access authorization status. [Note: This requirement does not preclude a contractor from having an employee execute a "Security Termination Statement" or restricting an employee's access to classified information or matter, or SNM, before notifying the DOE CSA.] DOE employees authorized to render access authorization eligibility determinations must receive training in the DOE personnel security process prior to actually rendering such determinations.

- Favorable and unfavorable investigative information must be analyzed according to the criteria found in 10 CFR 710.8, "Criteria." Frequently, the reported derogatory information alone raises a security concern but may be resolved when considered with other reported mitigating information.
- When information contained in investigative reports or the receipt of other reliable information raises a question concerning an individual's eligibility for an access authorization, additional actions may be authorized for collecting relevant information pertaining to the eligibility determination.

- If an investigation is complete, the authorized DOE employee (as defined in DOE M 470.4-5, chapter III, paragraph 2) may grant or continue an access authorization based on the existing record if: the file is clear of derogatory information; the post-investigative record fully mitigates any derogatory information; or an interview and/or other supplementary fact-finding effort has resolved all security concerns documented in the record.
- DOE's final determination regarding the eligibility for an access authorization will be provided in writing or electronically to the employer or prospective employer who initiated the request.
- If it is determined by the DOE CSA that reported information falls within one or more of the categories in 10 CFR 710.8 and the case cannot be resolved locally, then the access authorization must be suspended or recommended for denial.
- Any case may be referred to the Director, Office of Security, for review and advice. Any case referred must reflect the rationale and recommendations for further action.

c. Describe the six types of investigations most frequently conducted for the DOE.

The following is taken from DOE M 470.4-5.

The following are the types of investigation most frequently conducted for the DOE:

- SSBI is a full-field background investigation covering the most recent ten years of the individual's life.
- SSBI-PR is a background investigation covering the most recent five years of the individual's life.
- NACLC is a name check of the individual at appropriate Federal and local LEAs, a credit search, and a classification of the individual's fingerprints by the FBI.
- ANACI is a name check of the individual at appropriate Federal and local LEAs; a classification of the individual's fingerprints by the FBI; a credit search; and written inquiries regarding the individual's employment, education, residences, and references.
- Upgraded investigation—the type of investigation requested may be upgraded to a more extensive investigation if the case appears to involve significant derogatory issues.
- Background investigation by other Federal agencies must be accepted in lieu of a new investigation provided that: the investigation meets the scope and extent of the required investigation; and the investigation was completed, or upgraded by reinvestigation, within the most recent five years.

d. Discuss the tasks associated with the processing of a change to spouse/cohabitant form submitted by personnel with a "Q" or "L" clearance.

The following is taken from DOE M 470.4-5.

Access authorization applicants and holders must provide two completed copies of DOE F 5631.34, *Data Report on Spouse/Cohabitant*, directly to the processing personnel security

office, within forty-five working days, of marriage or cohabitation. Note: A cohabitant is a person who lives with the individual in a spouse-like relationship or with a similar bond of affection, but is not the individual's legal spouse, child, or other relative (in-laws, mother, father, brother, sister, etc.).

For an individual holding or applying for a "Q" access authorization whose new spouse or cohabitant is either a foreign national or a dual citizen, an Office of Personnel Management (OPM) National Agency Check (without fingerprint cards) will be requested on the new spouse or cohabitant by submitting two copies of the DOE F 5631.34 and a completed Office of Federal Investigations (OFI) 86C, *Special Agreement Checks*. The OFI 86C should be overprinted with the current agency agreement number and "S" should be entered in box 7 of the form.

For an individual holding or applying for an "L" access authorization whose new spouse or cohabitant is either a foreign national or a dual citizen, the DOE F 5631.34 should be forwarded to the Office of Security, which will arrange for the appropriate indices check.

e. Discuss the extension, transfer, termination, and reinstatement of access authorizations.

The following is taken from DOE M 470.4-5.

Extension

Extension of an access authorization is the process that allows an individual to hold concurrent active access authorizations under the cognizance of two or more departmental elements, two or more employers, or one employer under two or more contract numbers.

- A Q access authorization can be extended as either a Q or an L access authorization, but an L access authorization can be extended only as an L. An access authorization must not be extended to a departmental element where the individual is not employed or does not perform contractual duties.
- QX and LX access authorizations cannot be extended as they are granted for limited access as specified in an access permit.
- When derogatory information develops after an access authorization has been extended, the processing personnel security office in possession of the new information must notify all offices having an access authorization interest in the individual.
- In extensions, the processing personnel security office that granted the oldest active access authorization must be indicated on the CPCI as being the PSF location and will be responsible for the reinvestigation. The only exception is when the subsequent access authorization extension results in a higher type of access authorization.
- If the processing personnel security office that originated the access authorization terminates the access authorization, the PSF must be sent to the processing personnel security office to which the access authorization had been extended as described in DOE M 470.4-5, chapter VII, paragraph 4.

Transfers

Transfer of an access authorization requires a personnel security office to accept the active access authorization granted by another personnel security office simultaneously with the termination of that access authorization by the latter.

- In transfer cases, the PSF must be sent to the processing personnel security office to which the access authorization has been transferred as described in DOE M 470.4-5, chapter VII, paragraph 4. The PSF must be reviewed and documented upon receipt.
- When supplemental investigation is deemed appropriate, a request for such an investigation must be submitted to the appropriate investigative agency by the processing personnel security office to which the access authorization has been transferred.

A request for extension or transfer of an access authorization must contain the full name of the individual, date of birth, social security number, and DOE file number to establish positive identification.

The departmental element having custody of the individual's PSF must inform the personnel security office accepting the extension or transfer of the following:

- The individual's date of birth
- The individual's access authorization status
- The type of investigation upon which the access authorization was based
- If reinvestigated, the date and action taken
- Whether the PSF contains unresolved derogatory information

After positive identification has been established, and based on the information received, the individual's access authorization must be extended or accepted for transfer within two working days of receipt of all necessary information, unless the PSF contains unresolved derogatory information. The processing personnel security office having knowledge of unresolved derogatory information must notify all other offices having an access authorization interest in the individual of the details of the derogatory information.

If an access authorization is extended or transferred to a position certified as being "of a high degree of importance or sensitivity" and the previous investigation was not conducted by the FBI, the request for the new investigation, accompanied by a new SF 86, must be forwarded to the FBI.

The personnel security office extending the access authorization and the personnel security office accepting the transfer of an access authorization must update the CPCI accordingly. Interim access authorizations may be extended or transferred among processing personnel security offices.

Terminations

Within two working days of receipt of notification that an individual no longer requires access to classified information or matter, or SNM, DOE must terminate the individual's access authorization.

An access authorization must be terminated when there is termination of employment or change of official duties so that the position no longer requires access to classified information or matter, or SNM. Continuation may be authorized by the processing personnel security office when the employer has certified that the individual will be reemployed or reassigned to a position that requires an access authorization within 3 months and that DOE will be kept informed of the individual's status. The access authorization must be terminated if the holder is on leave of absence or extended leave and will not require access for at least 90 working days.

When an individual no longer requires an access authorization, or when an access authorization is administratively terminated, the processing personnel security office must be notified electronically or verbally within two working days to be followed by a completed DOE F 5631.29, *Security Termination Statement*. Within two working days of receipt of a DOE F 5631.29 or written notice of termination, the processing personnel security office must note in the individual's PSF the date the access authorization was actually terminated and must enter the appropriate information in the CPCI.

When an access authorization is to be terminated as required in DOE M 470.4-5, chapter VII, paragraph 2.a.(2), due to foreign travel not involving official U.S. government business, the individual must be advised that the access authorization is being terminated, the reason, and that it may be reinstated when the individual resumes work requiring it.

Reinstatements

A new or updated and recertified SF 86 must be obtained if more than 6 months have elapsed since termination of the access authorization and more than 1 year has elapsed since the date of the previous form, or when any significant changes are known to have occurred since that date. When an SF 86 is not required, a request for reinstatement must contain the date of birth of the individual to establish positive identification. A new DOE F 5631.18 must be obtained in all cases.

The individual's PSF must be reviewed against the new or updated SF 86 and identifiers such as full name, social security number, and date of birth compared to ensure that the individual being reinstated is the same person whose file is being reviewed. Supplemental investigation must be requested before, or concurrent with, reinstatement when any of the following conditions exist:

- The most recent investigation is more than five years old.
- The previous access authorization has been terminated for more than twenty-four months (unless the individual has been continuously employed by the same employer

where access authorization was held, in which case the access authorization can be reinstated for up to 5 years from termination).
- New derogatory information has been found and has not been resolved following the initial granting of the access authorization.
- The reason for the termination concerned eligibility for an access authorization.

If conditions described in DOE M 470.4-5, chapter VII, paragraphs c(3) or (4) exist and there is sufficient available information to proceed directly to AR processing, it is not necessary to schedule supplemental investigations. Supplemental investigation must be completed and adjudicated before reinstatement in any instance when more than ten years have elapsed since the previous investigation.

In requesting supplemental investigation, a completed SF 86 must be forwarded to the appropriate investigative agency. If a fingerprint card has been previously classified by the FBI, it is not necessary to submit a new fingerprint card.

Where the reinstatement involves assignment of an individual to a "position of a high degree of importance or sensitivity," and the previous investigation was not conducted by the FBI, a new SF 86 must be forwarded to the FBI for investigation.

f. Describe the reinvestigation program.

The following is taken from DOE M 470.4-5.

Except as authorized by the Director, Office of Security, individuals with access authorization must be periodically reinvestigated. Reinvestigations are designed to ensure that individuals with access authorizations are periodically reevaluated to determine their continued need for such access authorizations and reinvestigated to determine their continued eligibility. A reevaluation and reinvestigation must be completed every five years for individuals holding Q access authorizations and every ten years for individuals holding L access authorizations.

A review of the individual's eligibility for continuation of the access authorization must be based upon evaluation of: the individual's updated security forms; the individual's PSF; the completed investigation as described below; and any additional data resulting from required further investigative or administrative effort.

The type of reinvestigation to be conducted is determined by the type of access authorization held by the individual and the certification by the individual's sponsor of the individual's continued need for access. If an individual's SF 86 or PSF reflects new and/or unresolved derogatory information, the type of reinvestigation may be upgraded to resolve issues. Fingerprint cards are required only if there has not been a previously valid technical check by the FBI.

Q access authorization—at each five-year interval following completion of the previous investigation or reinvestigation, an SSBI-PR must be conducted. The investigation may be expanded or upgraded to resolve issues.

L access authorization—at each ten-year interval following completion of the previous investigation or reinvestigation, an NACLC must be conducted. The investigation may be expanded or upgraded to resolve issues.

The processing personnel security office must establish a schedule for submitting requests for reinvestigations for cases within their cognizance. Reinvestigations should be submitted to the investigative agency at even intervals throughout the year. A reinvestigation may be scheduled whenever there is evidence that the individual has engaged in an activity or has been subject to circumstances that cause a security concern within the meaning of 10 CFR 710 or as a follow-up to previously adjudicated derogatory issues. Processing security offices are authorized to request updated security forms to process a periodic reinvestigation or at any time there is probable cause to believe that the individual may have engaged in an activity, or been subject to circumstances, that affect continued eligibility for access authorization.

The results of the reinvestigation must be reviewed and adjudicated following the procedures in DOE M 470.4-5, chapter III for initial investigations. When a reinvestigation report contains derogatory information and the individual has an active access authorization, the case must receive priority processing to resolve the derogatory information as quickly as possible or to determine whether the individual's case warrants processing under AR procedures. The results of the evaluation must be entered into the CPCI. If an access authorization has been extended, the processing personnel security office must immediately notify any other DOE personnel security office or Federal agency where the individual holds an access authorization or security clearance of any unresolved derogatory information.

48. Safeguards and security personnel with the responsibility for PERS SEC must demonstrate the ability to assess the PERS SEC program elements.

a. Discuss the procedures used to assess the effectiveness of the DOE or contractor strategies for maintaining the minimum number of access authorizations consistent with operational efficiency.

The following is taken from DOE M 470.4-5.

DOE M 470.4-5 establishes the overall objectives and requirements for the personnel security program in DOE, including the NNSA. Its objectives include the following:

- To affect the policy in DOE P 470.1 by integrating personnel security into DOE operations as determined by line management, according to sound risk management practices.

- To ensure that individuals are processed for, granted, and allowed to retain an access authorization only when their official duties require access to classified information or matter, or SNM.
- To allow access to DOE classified information or matter, or SNM, only when it has been determined that such access will not endanger the common defense and security and is clearly consistent with the national interest.
- To maintain the numbers and types of access authorizations at the minimum levels necessary to ensure the operational efficiency of DOE programs and operations involving classified information or matter, or SNM.
- To conduct personnel security activities in a manner that ensures:
  - timely and efficient processing of initial access authorization requests and reinvestigations;
  - consistent, objective, and fair interpretation and application of criteria and procedures in every access authorization action;
  - timely review and adjudication of investigative reports and other information related to an individual's access authorization eligibility; and
  - maintenance of accurate, complete, and timely access authorization file and record information, the availability of such information to authorized users, and the protection of such information from unauthorized disclosure.
- To periodically evaluate individuals retaining access authorization to confirm their continued need for access and access authorization eligibility.
- To ensure that DOE employees, contractors, and others involved in personnel security activities effectively and efficiently execute their personnel security responsibilities.
- To prevent the use of personnel security activities for reprisal, discrimination, or any other unauthorized purpose.
- To promote proactive participation in personnel security activities at the international, national, and interagency levels to ensure the adequate expression and consideration of DOE mission and program interests.

b. Discuss methods used to determine the effectiveness of management and operating contractor pre-employment checks conducted in accordance with the DEAR.

The following is taken from DOE M 470.4-5.

Pre-Employment and Pre-Processing Requirements

The following statement must be included in advertisements for positions that require the selectees to be processed for an access authorization: "Applicants selected will be subject to a Federal background investigation and must meet eligibility requirements for access to classified information or matter."

The contractor must require applicants and employees selected for positions requiring access authorizations to provide evidence of U.S. citizenship and must verify such evidence to DOE when requesting that the individuals be processed for access authorizations. Acceptable

evidence of U.S. citizenship consists of: a birth certificate; a certificate of naturalization; a U.S. passport; a DD Form 1966, *Record of Military Processing-Armed Forces of the U.S.*; or for individuals claiming citizenship by birth to a U.S. citizen abroad, a Certificate of Citizenship issued by the Immigration and Naturalization Service, a Report of Birth Abroad of a Citizen of the U.S. of America (Form FS 240), or a Certificate of Birth (Form FS 545 or DS 1350).

When an access authorization will be required for an applicant or employee, the contractor must conduct the following checks to establish the individual's job qualifications and suitability before submitting the access authorization request to DOE:

- A credit check
- Verification of a high school degree or diploma or a degree or diploma granted by an institution of higher learning within the past five years
- Contacts with listed references
- Contacts with listed employers for the past three years
- Local law enforcement checks when such checks are not prohibited by state or local law, statute, or regulation, and when the individual has resided in the jurisdiction where the contractor is located

c. Discuss procedures for determining contractor compliance with requirements for timely notification of access authorization termination to the DOE.

The following is taken from DOE M 470.4-5.

The contractor must request that the DOE processing personnel security office(s) terminating an employee's access authorization must provide a DOE F 5631.29, completed by the employee whenever any of the following occur:

- Employment by the contractor is terminated
- An access authorization is no longer required
- The individual is on a leave of absence or an extended leave and will not require access to classified information or matter, or SNM, for ninety consecutive working days
- Access to classified information or matter, or SNM, is no longer required due to transfer to a position not requiring such access
- The individual leaves for foreign travel, employment, assignment, education, or residence of more than three months duration, not involving official U.S. government business, even if the individual remains employed by the contractor

The purpose of the DOE F 5631.29 is to ensure that the individual is aware of the continuing responsibility to protect classified information or matter after termination of an access authorization. The DOE processing personnel security office must be requested to terminate an employee's access authorization even though a completed DOE F 5631.29 cannot be immediately provided. In cases in which it is not possible to obtain the individual's signature, the completed but unsigned DOE F 5631.29 must still be submitted. In addition, the

contractor will provide an explanation to the DOE processing personnel security office of the circumstances surrounding the termination and why the signature could not be obtained.

d. Discuss the methods used in background investigations of funding estimates in response to budget calls.

The following is taken from 10 CFR 11.15.

OPM bills NRC for the cost of each background investigation conducted in support of an application for SNM access authorization. The combined cost of the OPM investigation and NRC's application processing overhead are recovered from the licensee through an MA authorization fee calculated with reference to current OPM personnel investigation billing rates (OPM rate + [(OPM rate x 31.7%), rounded to the nearest dollar] = NRC access authorization fee). Updated OPM billing rates are published periodically in a Federal Investigations Notice issued by OPM's Investigations Service. Copies of the current OPM billing schedule can be obtained by phoning the NRC's Personnel Security Branch, Division of Facilities and Security, Office of Administration. Any change in the NRC's access authorization fees will be applicable to each access authorization request received on or after the effective date of OPM's most recently published investigations billing schedule.

49. Safeguards and security personnel with the responsibility for PERS SEC must demonstrate a working level knowledge of all aspects and actions required of the access authorization process.

a. Describe the tasks associated with processing access authorization requests for access to classified matter or SNM.

The following is taken from DOE M 470.4-5.

The tasks for processing access authorization requests for access to classified matter or SNM are:

- A request for an access authorization will be processed only when the need for access is clearly justified and it is for the type (Q or L) required.
- Check for required documentation.
- Check forms to ensure they are filled out correctly, that all required forms are included, and to make sure that the form has not been altered.
- Check individual's citizenship.
- Determine if the individual requires a new background check. Q clearances must be reinvestigated ever five years and L clearances every 3 years.
- Determine the type of investigation required and have the applicant fill out the correct forms to start the investigation process.
- After receiving the completed investigation report, determine that the required DOE scope of investigation for the particular type of access authorization has been met and that all derogatory and mitigating information has been identified.

- If the investigation is determined to be complete, an access authorization may be issued to the applicant.
- If the investigation is determined not to be complete, it is forwarded for AR and the access authorization is suspended until review is completed.

b. Describe the tasks associated with downgrading, transferring, or extending an access authorization for access to classified matter or SNM.

The following is taken from DOE M 470.4-5.

The tasks associated with downgrading, transferring, or extending an access authorization for access to classified matter or SNM are:

- Check the request to ensure it contains the full name of the individual, date of birth, social security number, and DOE file number to establish positive identification.
- Inform the personnel security office accepting the application of the above information.
- There are two working days from receipt of all necessary information to extend or accept for transfer.
- If an access authorization is extended or transferred to a position certified as being "of a high degree of importance or sensitivity" check to ensure the previous investigation was conducted by the FBI. If not, forward the request to the FBI with a new SF 86.
- The personnel security office extending the access authorization and the personnel security office accepting the transfer of an access authorization must update the Central Personnel Clearance Index (CPCI) accordingly.
- Downgrades are handled in this same task structure except the request must be accompanied by a revised access authorization justification statement.

c. Describe the tasks associated with ensuring a reinvestigation is completed.

The following is taken from DOE M 470.4-5.

The tasks associated with ensuring a reinvestigation is completed are:

- Check the individual's eligibility for continuation of the access authorization based on evaluating
  - the individual's updated security forms;
  - the individual's PSF;
  - the completed investigation; and
  - any additional data resulting from required further investigative or administrative effort (e.g., personnel security interview, psychiatric evaluation, letter of interrogatory, and/or specialized indices checks).
- Determine the type of reinvestigation to be conducted by the type of access authorization held by the individual and the certification by the individual's continued need for access validated by their sponsor.
  - Q access authorization—at each five-year interval, an SSBI-PR must be conducted.

- L access authorization—at each ten-year interval, an NACLC must be conducted.

- Ensure the processing personnel security office schedules the reinvestigation.
- Ensure the results of the reinvestigation are reviewed and adjudicated.
- If there is derogatory information that has not been resolved, determine if the case warrants processing under the AR procedures; if so, enter into the CPCI.
- If access authorization is extended, issue new access authorization.

d. Discuss the tasks associated with terminating an access authorization.

The following is taken from DOE M 470.4-5.

The tasks associated with terminating an access authorization are:

- Notify the personnel security office, electronically or verbally, of the individual's termination and follow up with a completed DOE F 5631.29.
- Within two working days of receipt of DOE F 5631.29, the processing personnel security office must note in the individual's PSF the date the access authorization was actually terminated.
- Enter the appropriate information in the CPCI.
- If the access authorization is terminated due to foreign travel not involving official U.S. government business, the individual must be advised that the access authorization is being terminated, the reason, and that it may be reinstated when the individual resumes work requiring it.

e. Discuss the tasks associated with the processing of a change to spouse/cohabitant form submitted by personnel with a "Q" or "L" clearance.

The following is taken from DOE M 470.4-5.

The tasks associated with the processing of a change to spouse/cohabitant form submitted by personnel with a "Q" or "L" clearance are:

- For an individual applying or holding a "Q" access authorization whose new spouse or cohabitant is either a foreign national or a dual citizen, ensure that OPM National Agency Check (without fingerprint cards) is requested on the new spouse or cohabitant.
- Ensure two copies of the DOE F 5631.34 and a completed OFI 86C, overprinted with the current agency agreement number and "S" entered in box 7 of the form is submitted.
- For an individual holding or applying for an "L" access authorization whose new spouse or cohabitant is either a foreign national or a dual citizen, ensure the DOE F 5631.34 is forwarded to the Office of Security, which will arrange for the appropriate indices check.

f. Discuss the tasks associated with processing a Report of Investigation (ROI).

The following is taken from DOE M 470.4-5.

The tasks associated with processing a ROI are:

- When received, review it to ensure that the required DOE scope of investigation for the particular type of access authorization has been met and all derogatory and mitigating information has been identified.
- Send the ROI to be analyzed by qualified DOE employees authorized to render access authorization eligibility determinations.
- If unfavorable investigative information is found, the ROI is sent to adjudication.
- If favorable information is found, an access authorization can be issued.
- Provide in writing or electronically to the employer or prospective employer, the final determination regarding the eligibility for an access authorization.
- This information may also be furnished to representatives of DOE contractors or to Federal agencies having an official interest in the individual.
- If the case cannot be resolved, then the access authorization must be suspended.

g. Describe the tasks associated with processing reconsiderations.

The following is taken from 10 CFR 710.32.

The tasks associated with processing reconsiderations are:

- If the manager, hearing officer, appeal panel, or the secretary grants or reinstates access authorization for an individual, it is reconsidered as a new AR.
- A report for reconsideration must be submitted in writing to the Deputy Chief for Operations, Office of Health, Safety and Security.
- Attach an affidavit setting forth in detail the new evidence or evidence of rehabilitation or reformation.
- If the individual's access authorization is not reinstated following the reconsideration, the individual will be advised by the Director, Office of Personnel Security, DOE headquarters in writing.
- Within thirty calendar days from the date of receipt of the notification that the access authorization is not reinstated, the individual may file a written request for a review of the decision by the appeal panel.

50. Safeguards and security personnel with the responsibility for PERS SEC must demonstrate a working level knowledge of all aspects and actions required of the PERS SEC adjudication process.

a. Describe the procedures for conducting a screening of requests for access to classified matter or SNM.

The following is taken from DOE M 470.4-5.

When an investigative report is received, a personnel security specialist must review it to ensure that the required DOE scope of investigation for the particular type of access authorization has been met and that all derogatory and mitigating information has been identified.

The report must be reviewed to ensure that thorough information is provided on the individual's residence, employment, education, and military service, and that checks of references, credit, and law enforcement have been completed.

All derogatory and mitigating information, as well as any missing elements of investigative coverage, must be documented with the date and signature of the reviewer. The individual's employer, as listed on the SF 86, must be checked against the employer as reported in the investigation to ensure they are identical; if not, a check will be conducted to determine if the reported employer has submitted a request for access authorization and if it has been approved for the same type of access authorization.

Cases for which the investigation is complete and no derogatory information has been reported must be appropriately documented. If the reviewer has been delegated authority in writing to grant an access authorization, the granting must be so noted in the file. Such verification of review will be documented by the date and signature of the reviewer on the DOE F 5631.16, *File Summary Sheet*, or equivalent.

Individuals screening these investigations must determine whether all items have been covered. Derogatory and mitigating information must be listed and documented with the date and signature of the screener. If there is no derogatory information, the procedures listed in DOE M 470.4-5, chapter III, paragraph 1.a(3) should be followed.

b. Describe the evaluation (second review) process.

The following is taken from DOE M 470.4-5.

The results of the reinvestigation must be reviewed and adjudicated following the procedures in DOE M 470.4-5, chapter III for initial investigations. When a reinvestigation report contains derogatory information and the individual has an active access authorization, the case must receive priority processing to resolve the derogatory information as quickly as possible or to determine whether the individual's case warrants processing under AR procedures. The results of the evaluation must be entered into the CPCI. If an access authorization has been extended, the processing personnel security office must immediately notify any other DOE personnel security office or Federal agency where the individual holds an access authorization or security clearance of any unresolved derogatory information.

c. Discuss the processing of a Letter of Interrogatory (LOI).

The following is taken from DOE M 470.4-5.

An alternative to a personnel security interview (PSI) is the LOI, which may be sent to an individual if the derogatory information requires clarification, or if the geographic location of the individual would make it extremely difficult to arrange a PSI. Letters of interrogatory must include a deadline for the individual to provide the response. The individual's response will be evaluated to determine whether the security concern that prompted the letter was

resolved. If the individual's response does not favorably resolve the security concern, further adjudicative action must be taken.

d. Discuss the methods for conducting a Personnel Security Interview (PSI).

The following is taken from DOE M 470.4-5.

PSIs must be conducted only by personnel security specialists appropriately trained and cognizant of all the questions or items of information to be explored. DOE F 5631.5, *The Conduct of Personnel Security Interviews Under DOE Security Regulation*, and DOE F 5631.7, *Privacy Act Statement for Personnel Security Interviews and Release Forms Related Thereto*, must be properly executed for all PSIs. All PSIs will be audio or audio/video recorded. The PSI will then be transcribed or summarized. If a transcript is not prepared, the recorded PSI must be retained and protected in the same manner as the PSF.

e. Describe the process used in coordinating a mental evaluation.

The following is taken from DOE M 470.4-5.

To assist in determining whether reported information about a mental illness or condition falls within 10 CFR 710.8, the following procedures will be implemented:

- A DOE or contractor supervisor must report to the processing personnel security office when an individual under their cognizance, who holds an access authorization, is hospitalized for mental illness or receives other treatment for a condition that, in the supervisor's opinion, may cause a significant defect in the individual's judgment or reliability. Verbal notification must be made within eight working hours, and written confirmation within the next ten working days. The individual's access authorization will be continued unless the processing personnel security office finds convincing evidence that there is a significant defect in the individual's judgment or reliability as described in 10 CFR 710.8(h).
- To aid in determining the individual's judgment or reliability, the processing personnel security office may accept previously rendered competent medical advice or records that are in the possession of DOE or a DOE contractor. The processing personnel security office may also have a board-certified psychiatrist or a licensed clinical psychologist designated by DOE conduct a mental evaluation. Any referral to a DOE-designated psychiatrist or psychologist must be approved by the head of the processing security office. In such a case, the individual will be requested to submit to an examination and to execute a consent form (DOE F 5631.10, *Waiver*) for the examination.
    - The examining psychiatrist or psychologist must submit to the processing personnel security office a written report containing an opinion on whether the individual suffers from a mental illness or condition that causes or may cause a significant defect in judgment or reliability.

- If the individual refuses to submit to an examination, the individual's access authorization may be terminated according to 10 CFR 710.6, "Cooperation by the individual."

- If a psychiatric or psychological examination is conducted as described in DOE M 470.4-5, chapter III, paragraph 8.b, the DOE-designated examiner must be notified that they may be called upon to testify before a hearing officer. Only psychiatrists or psychologists consenting to testify should be designated for examining purposes.

f. Describe the processing of a suspension.

The following is taken from DOE M 470.4-5.

Upon receipt of notification by the DOE processing personnel security office of an employee's access authorization suspension, the contractor must ensure that the employee is precluded from access to classified information or matter, or categories of SNM, requiring an access authorization. When the security issue(s) concerning the employee's access authorization status has been resolved, the contractor will be notified in writing by the DOE processing personnel security office of whether the employee's access authorization has been reinstated, revoked, or denied.

Suspension of an individual's access authorization does not preclude the contractor from assigning or transferring the individual to duties that do not require an access authorization.

51. Safeguards and security personnel with the responsibility for PERS SEC must demonstrate a working level knowledge of all aspects and actions required of the AR process.

a. Describe the processing of an AR.

The following is taken from 10 CFR 710.21.

The processing of an AR consists of:

- Unless an extension is authorized within 30 calendar days of receipt of authority to institute AR procedures, the manager shall prepare and deliver to the individual a notification letter approved by the local Office of Chief Counsel. Where practicable, the letter shall be delivered to the individual in person.
- The letter shall state
  - that reliable information in the possession of DOE has created a substantial doubt concerning the individual's eligibility for access authorization;
  - the information which creates a substantial doubt regarding the individual's access authorization eligibility; and
  - that the individual has the option to have the substantial doubt regarding eligibility for access authorization resolved in one of two ways:

- by the manager, without a hearing, on the basis of the existing information in the case; or
- by personal appearance before a hearing officer.

- that, if the individual desires a hearing, the individual must, within twenty calendar days of the date of receipt of the notification letter, indicate this in writing to the manager from whom the letter was received;
- that the individual may also file with the manager the individual's written answer to the reported information which raises the question of the individual's eligibility for access authorization, and that, if the individual requests a hearing without filing a written answer, the request shall be deemed a general denial of all the reported information;
- that, if the individual so requests, a hearing will be scheduled before a hearing officer, with due regard for the convenience and necessity of the parties or their representatives, for the purpose of affording the individual an opportunity of supporting his eligibility for access authorization;
- that, if a hearing is requested, the individual will have the right to appear personally before a hearing officer; to present evidence in his own behalf, through witnesses, or by documents, or both; and, subject to the limitations set forth in 10 CFR 710.26(g), "Conduct of Hearings," to be present during the entire hearing and be accompanied, represented, and advised by counsel or representative of the individual's choosing and at the individual's own expense;
- that the individual's failure to file a timely written request for a hearing before a hearing officer according to 10 CFR 710.22, "Initial Decision Process," paragraph (b)(4) of this section, unless time deadlines are extended for good cause, will be considered as a relinquishment by the individual in this subpart, and that in such event a final decision will be made by the manager; and
- that in any proceedings under this subpart DOE counsel will be participating on behalf of, and representing DOE, and that any statements made by the individual to DOE counsel may be used in subsequent proceedings.

b. Discuss the tasks associated with participating in an AR hearing.

The following is taken from 10 CFR 710.26 and 27.

The tasks associated with participating in an AR hearing are:

- The individual will select a person to represent him.
- The individual will produce witnesses in their own behalf, including requesting issuance of subpoenas.
- Hearings are open only to DOE counsel; duly authorized representatives of the staff of DOE, the individual and his counsel or representative, and such other persons as may be authorized by the hearing officer.
- The individual shall be afforded the opportunity of presenting evidence.
- All witnesses are subject to cross-examination, if possible.
- The hearing officer may ask witnesses questions.

- The hearing officer shall rule on all questions presented to the hearing officer.
- The hearing officer shall ensure that classified materials are not disclosed to persons who are not authorized to receive it.
- Testimony of the individual and witnesses shall be given under oath or affirmation.
- The hearing officer shall endeavor to obtain all the facts that are reasonably available in order to arrive at findings.
- Oral or written statements may be received and considered by the hearing officer.
- A written transcript of the entire proceedings shall be made and, except for portions containing RD or NSI, a copy shall be furnished to the individual without cost.
- The hearing officer shall carefully consider the record in view of the standards set forth herein and shall render a decision as to whether the grant or restoration of access authorization to the individual would not endanger the common defense and security and would be clearly consistent with the national interest.

c. Describe the tasks associated with taking actions following an AR hearing.

The following is taken from 10 CFR 710.28.

The tasks associated with taking actions following an AR hearing are:

- Within ten calendar days of receipt of the decision and the administrative record, unless an extension of time is granted by the Director, Office of Personnel Security, DOE headquarters, the manager shall
  - notify the individual in writing of the hearing officer's decision;
  - advise the individual in writing of the appeal procedures available to the individual in 10 CFR 710.28(b), "Action on the Hearing Officer's Decision," if the decision is unfavorable to the individual;
  - advise the individual in writing of the appeal procedures available to the manager and the Director, Office of Personnel Security, DOE headquarters, in 10 CFR 710.28(c) if the decision is favorable to the individual; and
  - provide the individual and/or counsel or representative, a copy of the hearing officer's decision and the administrative record.
- If the hearing officer's decision is unfavorable to the individual
  - the individual may file with the Director, Office of Personnel Security, DOE headquarters, a written request for further review of the decision by the appeal panel along with a statement required by 10 CFR 710.28(e) within thirty calendar days of the individual's receipt of the manager's notice;
  - the Director, Office of Personnel Security, DOE headquarters may, for good cause shown, extend the time for filing a request for further review of the decision by the appeal panel at the written request for an extension of time filed by the individual within thirty calendar days of receipt of the manager's notice;
  - the hearing officer's decision shall be considered final if the individual does not:

- file a written request for a review of the decision by the appeal panel or for an extension of time to file a written request for further review of the decision by the appeal panel according to 10 CFR 710.28(b)(1) or (b)(2); or
- file a written request for a further review of the decision by the appeal panel after having been granted an extension of time to do so.

- If the hearing officer's decision is favorable to the individual, within 30 calendar days of the individual's receipt of the manager's notice
  - the manager or the Director, Office of Personnel Security, DOE headquarters, may file a written request for further review of the decision by the appeal panel along with the statement required by 10 CFR 710.28(e);
  - the Deputy Chief for Operations Office of Health, Safety and Security, may, at the written request of the manager or Director, Office of Personnel Security, DOE headquarters, extend the time for filing a request for further review of the decision by the appeal panel; or
  - the manager, with the concurrence of the Director, Office of Personnel Security, DOE Headquarters, shall grant or reinstate the individual's access authorization.
- A copy of any request for further review of the individual's case by the appeal panel filed by the manager or the Director, Office of Personnel Security, shall be provided to the individual by the manager.
- The party filing a request for review of the individual's case by the appeal panel shall include with the request a statement identifying the issues on which it wishes the appeal panel to focus. A copy of such statement shall be served on the other party, who may file a response with the appeal panel within twenty calendar days of receipt of the statement.

52. Safeguards and security personnel with the responsibility for PERS SEC must demonstrate a working level knowledge of the HRP.

a. Describe the purpose of the HRP.

The following is taken from 10 CFR 712.1.

The HRP is a security and safety reliability program designed to ensure that individuals who occupy positions affording access to certain materials, nuclear explosive devices, facilities, and programs meet the highest standards of reliability and physical and mental suitability. This objective is accomplished under this part through a system of continuous evaluation that identifies individuals whose judgment and reliability may be impaired by physical or mental/personality disorders, alcohol abuse, use of illegal drugs or the abuse of legal drugs or other substances, or any other condition or circumstance that may be of a security or safety concern.

b. Describe the process for identifying or removing positions from the HRP.

Identifying

The following is taken from 10 CFR 712.10.

HRP certification is required for each individual assigned to, or applying for, a position that

- affords access to category I SNM or has responsibility for transportation or protection of category I quantities of SNM;
- involves nuclear explosive duties or has responsibility for working with, protecting, or transporting nuclear explosives, nuclear devices, or selected components;
- affords access to information concerning vulnerabilities in protective systems when transporting nuclear explosives, nuclear devices, selected components, or category I quantities of SNM;
- is not included in 10 CFR 712.10, "Designation of HRP Positions," paragraphs (a)(1) through (3); but affords the potential to significantly impact national security or cause unacceptable damage and is approved pursuant to 10 CFR 712.10, paragraph (b).

The manager or HRP management official may nominate positions for the HRP that are not specified in 10 CFR 712.10, paragraphs (a)(1) through (3) or that have not previously been designated HRP positions. All such nominations must be submitted to and approved by either the NNSA administrator, his or her designee, the Chief, Health, Safety and Security Officer, or the appropriate lead program secretarial office, or his or her designee.

Immediate Removal

The following is taken from 10 CFR 712.19.

A supervisor who has a reasonable belief that an HRP-certified individual is not reliable, based on either a safety or security concern, must immediately remove that individual from HRP duties pending a determination of the individual's reliability. A supervisor must immediately remove an individual from HRP duties when requested to do so by the HRP certifying official. The supervisor must, at a minimum

- require the individual to stop performing HRP duties
- take action to ensure the individual is denied both escorted and unescorted access to the MAA
- provide, within twenty-four hours, to the individual and the HRP management official, a written reason for these actions

Temporary Removal

The following is taken from 10 CFR 712.19.

If an HRP management official receives a supervisor's written notice of the immediate removal of an HRP-certified individual, that official must direct the temporary removal of the individual pending an evaluation and determination of the individual's reliability. If removal is based on a security concern, the HRP management official must notify the HRP certifying

official and the applicable DOE personnel security office. The security concern will be resolved under the criteria and procedures in 10 CFR 710, subpart A, "appendix A to subpart A of part 710—Selected Provisions of the Atomic Energy Act of 1954, as amended, section 141 (42 U.S.C. 2161), section 145 (42 U.S.C. 2165), and section 161 (42 U.S.C. 2201)."

If removal is based on a concern that is not security related, the HRP management official must conduct an evaluation that led the supervisor to remove the individual from HRP duties. The HRP management official must prepare a written report of the evaluation that includes a determination of the individual's reliability for continuing HRP certification. If the management official determines that an individual who has been temporarily removed continues to meet the requirements for certification, the HRP management official must: notify the individual's supervisor of the determination and direct that the individual be allowed to return to HRP duties; notify the individual; and notify the HRP certifying official.

If the HRP management official determines that an individual who has been temporarily removed does not meet the HRP requirements for certification, the HRP management official must forward the written report to the HRP certifying official. If the HRP certifying official is not the manager, the HRP certifying official must review the written report and take one of the following actions: direct that the individual be reinstated and provide written explanation of the reasons and factual bases for the action; direct continuation of the temporary removal pending completion of specified actions to resolve the concerns about the individual's reliability; or recommend to the manager the revocation of the individual's certification and provide written explanation of the reasons and factual bases for the decision.

The manager, on receiving the HRP management official's written report and the HRP certifying official's recommendation (if any), must take one of the following actions: direct reinstatement of the individual, direct revocation of the individual's HRP certification, or direct continuation of the temporary removal pending completion of specified action to resolve the concerns about the individual's reliability.

If the action is revocation, the manager must provide the individual a copy of the HRP management official's report. The manager may withhold the report, or portions of the report, to the extent that he or she determines that the report, or portions of the report, may be exempt from access by the employee under the Privacy Act or the Freedom of Information Act.

If an individual is directed by the manager to take specified actions to resolve HRP concerns, he or she must be reevaluated by the HRP management official and HRP certifying official after those actions have been completed. After considering the HRP management and HRP certifying officials' report and recommendation, the manager must direct either reinstatement of the individual or revocation of the individual's HRP certification.

c. Describe the general requirements for HRP certification.

The following is taken from 10 CFR 712.11.

The following certification requirements apply to each individual applying for or in an HRP position:

- A DOE "Q" access authorization based on a background investigation, except for SPOs who have been granted an interim "Q" through the accelerated access authorization program
- The annual submission of SF 86, Office of Management and Budget (OMB) control number 3206-0007, Questionnaire for National Security Positions, part 2, and an annual review of the PSF
- Signed releases, acknowledgements, and waivers to participate in the HRP on forms provided by DOE
- Completion of initial and annual HRP instruction as provided in 10 CFR 712.17, "Instructional Requirements"
- Successful completion of an initial and annual supervisory review, medical assessment, management evaluation, and a DOE personnel security review for certification and recertification according to 10 CFR 712.11, "General Requirements for HRP Certification." With respect to the DOE personnel security review
  - if the DOE personnel security review is not completed within the twelve-month time period and the individual's access authorization is not suspended, the HRP certification form shall be forwarded to the HRP certifying official for recertification or temporary removal, contingent upon a favorable security review;
  - if a final determination has been made by DOE personnel security that is favorable, this information shall be forwarded to the HRP certifying official and so noted on the certification form; or
  - if the final determination has been made by DOE personnel security that the access authorization has been suspended, the individual shall be immediately removed from the HRP position, the HRP certifying official notified, the information noted on the certification form, and the procedures outlined in 10 CFR 710, subpart A, "Fees for Facilities, Materials, Import, and Export Licenses, and Other Regulatory Services Under the Atomic Energy Act of 1954, as amended," shall be followed.
- No use of any hallucinogen in the preceding 5 years and no experience of flashback resulting from the use of any hallucinogen more than 5 years before applying for certification or recertification
- A psychological evaluation consisting of a generally accepted psychological assessment (test) and a semi-structured interview
- An initial drug test and random drug tests for the use of illegal drugs at least once each twelve months according to DOE policies implementing EO 12564, *Drug-free Federal Workplace*, or the relevant provisions of 10 CFR 707, "Workplace Substance Abuse Programs at DOE Sites," for DOE contractors, and DOE Order 3792.3, *Drug-Free Federal Workplace Testing Implementation Program*, for DOE employees
- An initial alcohol test and random alcohol tests at least once each twelve months using an evidential-grade breath alcohol device, as listed without asterisks on the Conforming Products List of Evidential Breath Measurement Devices published by

the National Highway Traffic Safety Administration (49 CFR 40, "Procedures for Transportation Workplace Drug and Alcohol Testing Program")
- Successful completion of a CI evaluation, which includes a CI-scope polygraph examination according to DOE's Polygraph Examination Regulation, 10 CFR 709, "Counterintelligence Evaluation Programs," and any subsequent revisions to that regulation

F. NUCLEAR MATERIAL CONTROL AND ACCOUNTABILITY (MC&A)

53. Safeguards and security personnel with the responsibility for MC&A must demonstrate a working level knowledge of program administration of MC&A systems.

a. Describe the MC&A program for controlling and accounting for all identified nuclear materials and the prevention of theft and diversion of SNM.

The following is taken from DOE M 470.4-6 chg 1.

A nuclear MC&A program must be provided at DOE facilities and for DOE-owned materials at other facilities that are exempt from licensing by the NRC. DOE line management and site/facility operators must consider MC&A requirements, systems, technologies, and activities when planning, designing, constructing, and operating new or renovated DOE facilities. The site/facility operator must use techniques and equipment that maximize material loss detection sensitivity, increase the quality of accountability measurements, minimize material holdup, and reduce the magnitude of inventory differences and associated control limits consistent with the consequences of the loss of the material.

- An MC&A program must be established and maintained for all materials identified in DOE M 470.4-6, table I-1, *Nuclear Materials*. The level of control and accountability must be graded based on the consequence of their loss.
- SNM must not be received, processed, or stored at a facility until a facility approval has been granted.
- MC&A programs must be designed to deter and detect theft and diversion of nuclear material by both outside and inside adversaries.
- A performance-testing program to verify MC&A procedures and practices and to demonstrate that material controls are effective must be established.
- MC&A programs must address both the theft and diversion of SNM and the unauthorized control of a weapon, test device, or materials that can be used to make an improvised nuclear device.

b. Discuss the procedures in place for the prevention of the unauthorized control of a weapon, test device, or materials that can be used to make an improvised nuclear device.

The following is taken from DOE M 470.4-6 chg 1.

A reporting identification symbol (RIS) must be established for all nuclear material on inventory. A nuclear materials representative (NMR) must be designated for each site/facility with a RIS. The NMR is to be responsible for nuclear materials reporting and data submission to the Nuclear Materials Management and Safeguards Systems (NMMSS).

An MC&A plan providing the safeguards authorization basis must be developed and maintained for each facility possessing nuclear materials. The MC&A plan must specify how nuclear material inventory holdings will be accounted for and controlled. The MC&A plan must include, at a minimum

- the elements of the MC&A program that are designed to deter and detect loss, theft, and diversion of nuclear materials and the unauthorized control of a weapon, test device, or materials that can be used to make an improvised nuclear device;
- measures to ensure that nuclear materials are in their authorized locations and being used for their intended purposes;
- a description of the local implementation of DOE M 470.4-6 chg 1, which must document how the MC&A program meets the requirements of this manual;
- facility-specific requirements approved by the DOE CSA including, but not limited to, agreements between government and contractor organizations, access control and material surveillance testing measures, and the scope and extent of the performance-testing program; and
- MC&A plan review frequency and change control mechanisms.

c. Describe the procedures for receiving, processing, and storing of SNM at an approved facility.

The following is taken from DOE M 470.4-6 chg 1.

Immediately after receipt, shipments must be subjected to a transfer check. Transfer checks must consist of confirming the shipping container or item count, validating the tamper indicating device (TID) integrity and identification, verifying the tamper-indicating characteristics of the container, and comparing with shipping documentation to ensure the shipment was received intact. For external transfers, all SNM containers must be tamper-indicating.

For all unirradiated category I and II quantities of SNM transferred between facilities having a different RIS, the receiver must perform a verification or accountability measurement unless both RISs are located on the same site and are operated by the same site contractor. Both verification measurements and accountability measurements are quantitative measurements used by the receiver to verify that the amount of SNM in a shipment is as stated by the shipper. Accountability measurements differ from verification measurements only in how they are used in the receiver's accountability system. Accountability measurements are entered in receiver's accountability system as the value for the shipment. When verification measurements are used, the shipper's values are entered into the receiver's accountability records.

Controls must be established and implemented for each facility to ensure that nuclear materials are used, processed, or stored within a material balance area (MBA) and are controlled according to the graded safeguards concept. These controls must ensure that materials are removed only through authorized pathways or portals and are subject to transfer and verification procedures identified in DOE M 470.4-6 chg 1, section a, chapter II, paragraph 5. Controls for MBAs must meet the following:

- Be formally documented
- Identify geographical boundaries and functions of the MBA
- Identify material types, forms, and quantities permitted in each MBA
- Describe administrative controls for each MBA
- Define custodial responsibilities for nuclear materials contained within an MBA
- Identify personnel authorized to receive or ship nuclear material
- Identify material flow into and out of an MBA
- Ensure material transfer procedures are followed
- Ensure that material quantities transferred across MBA boundaries are based on measured values consistent with DOE M 470.4-6 chg 1, chapter II, paragraph 5b(5)

d. Describe the methods in place designed to deter and detect theft and diversion of nuclear material by both outside and inside adversaries.

The following is taken from DOE M 470.4-6 chg 1.

The methods in place to deter and detect theft and diversion of nuclear material by both outside and inside adversaries are:

- Loss detection evaluation—An assessment program for identifying and evaluating facility capability to detect the loss of category I quantities of SNM must be developed for each category I facility. Potential targets must include all category I and any other areas for which a credible scenario for unauthorized accumulation of a category I quantity of SNM have been identified. VAs must be approved by the DOE CSA and must be reviewed annually (at least every twelve months) and updated when there are system changes or new information indicates a potentially significant change in the risk of unauthorized removal of SNM.
- Performance testing—MC&A performance-testing programs must be developed and documented to support and verify loss detection capability and system effectiveness.

e. Discuss the performance testing program to verify MC&A procedures and practices and to demonstrate that material controls are effective.

The following is taken from DOE M 470.4-6 chg 1.

MC&A performance-testing programs must be developed and documented to support and verify loss detection capability and system effectiveness. The scope and intent of performance testing must be based on the graded safeguards concept.

- Performance tests must be designed to demonstrate that the MC&A system is functional and to ensure that the system performs as specified or required. The site/facility operator for the facilities must
  - identify those system components that provide the greatest effectiveness against theft and diversion;
  - design, conduct, and document tests that substantiate component effectiveness; and
  - integrate the results of these component tests into S&S risk management programs and VAs.
- The performance-testing program must include those elements that can detect a threat in time to prevent it and those elements that can effectively account for SNM to detect material loss and ensure that S&S systems are functioning properly. It must also focus on testing individual detection elements. Elements identified in a vulnerability assessment that contribute to detection capability must be tested on a frequency that is based on the level of risk.
- Performance testing must include testing to determine whether S&S systems have failed, including testing for loss of SNM. The accuracy of the accounting system and its capability to provide information about the quantity, location, and identifying characteristics of nuclear material, must be tested.
- Corrective action plans for systems that have failed performance testing must be developed and interim compensatory measures put in place.

f. Describe the use of the Reporting Identification Symbol (RIS) in the inventory of nuclear materials, and the methods for reporting and submitting data to the Nuclear Materials Management and Safeguards System (NMMSS).

The following is taken from DOE M 470.4-6 chg 1.

All RIS-level nuclear materials transactions, material balances, and inventories must be documented according to the instructions provided in DOE M 470.4-6 chg 1, section B and reported to the NMMSS.

The NMMSS will be used to accumulate and distribute information concerning nuclear materials transactions, material balances, and inventories. Submissions must be made in a timely manner to achieve reporting of accurate and complete data as soon as possible after the events described by the data.

The national database will provide nuclear materials information relating to safeguards, materials management and production, inventory quantities and valuations, and other information required by DOE and NRC. The database will serve as the centralized reporting facility to provide the information required under the provisions of the U.S./International Atomic Energy Agency (IAEA) safeguards agreement.

Data collection forms identified and described in DOE M 470.4-6 chg 1, chapter XVII (or the electronic equivalent) will be used to document and report nuclear materials transactions,

material balances, and inventories according to the instructions provided in this manual. A computer-generated form must contain all information necessary for proper documentation and reporting of nuclear materials transactions, material balances and inventories. Corrections of data previously submitted and found to be in error must be submitted to NMMSS within one working day following notification of the error.

g. Describe the authorities and responsibilities for the MC&A functions (e.g., account system, measurements, measurement control, inventories, audit, material access controls, and surveillance).

The following is taken from DOE M 470.4-6 chg 1.

Account System

A system for tracking nuclear material inventories, documenting nuclear material transactions, issuing periodic reports, and assisting with the detection of unauthorized system access, data falsification, and material gains or losses must be established according to the requirements of DOE M 470.4-6 chg 1, chapter II. The accounting system must provide a complete audit trail for all nuclear material from receipt through disposition. The site/facility operator must establish documented acceptance or rejection criteria for inventory confirmation and verification measurements based on valid technical and statistical principles.

Measurements and Measurement Control

Measurement and measurement control programs approved by the DOE CSA must be implemented at all facilities with nuclear material. Measurement programs used to determine category I or II inventories of SNM or used to determine a category I or II SNM throughput over a six-month period must meet the requirements set forth in DOE M 470.4-6 chg 1, chapter II, paragraphs 4a-4e. All measurement systems used for accountability purposes must have associated measurement control programs to ensure the quality of measurement data generated.

Measurement programs used to determine category III or IV inventories of SNM must address the topics set forth in DOE M 470.4-6 chg 1, chapter II, paragraphs 4a-4e; but the specific measurement and measurement control requirements will be determined by the DOE CSA.

Measurement systems used for accountability purposes must be precise and accurate enough to minimize the contribution of measurement error to the limit of error of the inventory difference. Nuclear materials not amenable to verification measurement must be identified in the facility's MC&A plan. Inventory values for these materials must be based on measured values or technically justified estimates. Justification and supporting documentation for these inventory values must be maintained and readily retrievable for review.

Inventories

The site/facility operator must establish documented acceptance or rejection criteria for inventory confirmation and verification measurements based on valid technical and statistical principles. For category I and II items, acceptance and rejection criteria must be consistent with performance requirements for confirmation and verification measurements shown in DOE M 470.4-6 chg 1, chapter I, paragraph 4c. The site/facility operator must prepare and implement a response plan for evaluating and resolving all verification and confirmation measurements that fail to meet acceptance criteria. Items that fail to meet the confirmation or verification measurement acceptance criteria must not be processed before the discrepancy is resolved.

Audit

The accounting system must provide a complete audit trail for all nuclear material from receipt through disposition. The authorities for audits are the same as for account systems.

Material Access Controls

A documented program must be established and implemented for each facility to ensure that only properly authorized personnel have access to nuclear materials. This program must address procedures and mechanisms to detect and respond to access by unauthorized personnel. To minimize the potential for unauthorized access to nuclear material, the amount of material in use must be limited to that necessary for operational requirements, and excess material must be stored in repositories or kept in enclosures designed to ensure that access will be limited to authorized individuals. Authority of this system is DOE M 470.4-6 chg 1, chapter III.

Surveillance

A nuclear materials surveillance program approved by the DOE CSA must be established and implemented for each facility. The program must ensure that nuclear materials are in their authorized locations, be capable of detecting unauthorized activities or anomalous conditions, and be capable of reporting material status. The surveillance program must address both normal and emergency conditions and include periodic testing. Authority for this system is DOE M 470.4-6 chg 1, chapter III.

h. Describe the contents and use of Table I-1, Nuclear Materials, contained in DOE M 470.4-6 chg 1, *Nuclear Material Control and Accountability*.

The following is taken from DOE M 470.4-6 chg 1.

Contents

DOE M 470.4-6 chg 1, table I-1, contains a listing of all the nuclear materials recognized by DOE M 470.4-6 chg 1; whether the material is SNM, source, or other; the reportable quantity, which is the minimum amount of material subject to the requirements of DOE M 470.4-6 chg 1; the weight field used for each element; the weight field used for each isotope; and the material type code.

Use

Each DOE facility must establish and maintain a nuclear MC&A program for all the materials listed in table I-1. The level of control and accountability must be graded based on the consequence of the loss of these materials.

i. Describe how nuclear material inventory holdings are accounted for and controlled.

The following is taken from DOE M 470.4-6 chg 1.

The MC&A plan must specify how nuclear material inventory holdings will be accounted for and controlled. The MC&A plan must include, at a minimum

- the elements of the MC&A program that are designed to deter and detect loss, theft, and diversion of nuclear materials and the unauthorized control of a weapon, test device, or materials that can be used to make an improvised nuclear device;
- measures to ensure that nuclear materials are in their authorized locations and being used for their intended purposes;
- a description of the local implementation of DOE M 470.4-6 chg 1, which must document how the MC&A program meets the requirements of DOE M 470.4-6 chg 1;
- facility-specific requirements approved by the DOE CSA including, but not limited to, agreements between government and contractor organizations, access control and material surveillance testing measures, and the scope and extent of the performance-testing program; and
- MC&A plan review frequency and change control mechanisms.

j. Explain the elements of the MC&A program that are designed to deter and detect loss, theft, and diversion of nuclear materials and the unauthorized control of a weapon, test device, or materials that can be used to make an improvised nuclear device. Discuss the measures used to ensure that nuclear materials are in their authorized locations and being used for their intended purposes.

The following is taken from DOE M 470.4-6 chg 1.

Systems must be in place to detect and assess the unauthorized removal of nuclear materials, consistent with the graded safeguards concept. The system must be interfaced with the facility's physical protection and other organizational systems, as appropriate, and must be able to detect and localize removal of SNM from its authorized location, and notify the PF and other organizations to respond when such events are detected.

A documented program, administered by the MC&A organization, must be in place to control TID and ensure that TIDs are used to detect violations of container integrity. TID programs cannot be regarded as effective unless used in conjunction with a material surveillance program. Testing of TID integrity, location, application, and the TID record system must be conducted. The TID control program must include the following elements:

- ID acquisition/procurement/destruction

- Types of TIDs used
- Unique TID identification
- Storage
- Issuance
- Personnel authorized to apply, remove, and dispose of TIDs
- Containers on which TIDs are to be applied
- Procedures for application of TIDs
- Frequency and method of TID verification
- Procedures for responding to, and reporting of TID violations
- Frequency and method of internal program audits
- A DOE CSA-approved listing of all containers considered to be intrinsically tamper-indicating

k. Describe the facility-specific requirements approved by the DOE CSA including, but not limited to, agreements between Government and contractor organizations, access control and material surveillance testing measures, and the scope and extent of the performance testing program.

This is a site-specific KSA. The Qualifying Official will evaluate its completion.

l. Discuss the MC&A plan review frequency and change control mechanisms.

The frequency of the MC&A plan review is determined by the DOE CSA. Change control mechanisms vary by site. The local Qualifying Official will evaluate the completion of the KSA.

m. Discuss the established procedures used by the site/facility operator for emergency conditions and periods when MC&A systems are inoperative, and explain the measures in place to ensure that access to or removal of SNM would be detected during these periods, and the control of SNM and measures to be taken before resuming operations following the emergency.

The following is taken from DOE M 470.4-6 chg 1.

Controls must be established to ensure detection equipment remains operational during emergency conditions. Detectors and calibration standards must be maintained and controlled to ensure that portal monitors are capable of meeting detection requirements. Periodic performance testing of portal monitors must be conducted according to DOE M 470.4-6 chg 1.

Procedures must be established by the site/facility operator for emergency conditions and periods when MC&A systems are inoperative. These measures must ensure that access to or removal of SNM would be detected during these periods. The MC&A plan must address control of SNM during emergency operations and measures to be taken before resuming operations following an emergency.

All liquid, solid, and gaseous waste streams leaving an MAA must be monitored to detect the theft or diversion of SNM. Facility waste-monitoring equipment must be maintained and controlled to ensure that the equipment is capable of detecting specified amounts of SNM as determined by the DOE CSA. Instrumentation used to monitor waste and equipment removed from an MAA must be able to detect, in combination with other detection elements, the removal of a category I quantity of SNM through a credible theft or diversion scenario.

A response plan for evaluating and resolving situations involving any discharge exceeding facility-specific limits must be established by the site/facility operator for the facility, and approved by the DOE CSA.

MC&A systems must be established for monitoring and control to provide the capability of detecting and assessing unauthorized SNM removals. Systems can include weight sensors, SNM/physical presence detectors, fiber optic seals, surveillance cameras, vault monitors, emergency egress radiation monitors, real-time inventory locator systems, etc. The MC&A system must provide sufficient information to correctly assess the alarms, localize the removal, and estimate the quantity and form of the diverted or stolen material.

Facilities must report data to the NMMSS electronically. If electronic means are unavailable, reporting using paper forms is permitted; however, it must be coordinated through the DOE CSA. Under emergency conditions or if a special, non-standard report is required, paper forms may be used.

n. Describe the policies and procedures for the termination of safeguards of nuclear materials that exempts nuclear materials from requirements of DOE M 470.4-6 chg 1, *Nuclear Material Control and Accountability.*

The following is taken from DOE M 470.4-6 chg 1.

Termination of safeguards exempts nuclear materials from requirements of DOE M 470.4-6 chg 1 and thereby removes the safeguards basis for applying physical protection requirements for theft and diversion of nuclear material, providing termination requirements are met as specified in DOE M 470.4-6 chg 1, section A, q.(1) and (2). Requirements for safeguards termination depend on the safeguards attractiveness levels of the material. Attractiveness levels are described in DOE M 470.4-6 chg 1, table I-4, *Graded Safeguards*.

Safeguards can be terminated on nuclear materials provided the following conditions are met:

- If the material is SNM or protected as SNM, it must be attractiveness level E and have a measured value.
- The material has been determined by DOE line management to be of no programmatic value to DOE. The radiological sabotage risks associated with the materials have been evaluated and additional measures beyond waste management regulations put in place to ensure that protection requirements, if applicable, will be met after safeguards termination. Only nuclear materials that are of radiological sabotage concern need to be evaluated against this requirement.

- The material is transferred to the control of a waste management organization where the material is accounted for and protected according to waste management regulations. The material must not be collocated with other accountable nuclear materials.
- In some cases, it may be necessary to dispose of nuclear materials of attractiveness level D or higher SNM. For DOE facilities, termination of safeguards for such materials must be approved by the departmental element after consultation with the Office of Security. For NNSA facilities, termination of safeguards for such materials must be approved by the Associate Administrator for Defense Nuclear Security, after consultation with the Office of Security.

o. Describe the policies and procedures for applying reduced safeguards to materials that both meet the criteria of Table I-3, Technical Criteria for Retained Waste, and have been removed from processing Material Balance Areas (MBAs).

The following is taken from DOE M 470.4-6 chg 1.

Reduced safeguards can be applied to materials that both meet the criteria of DOE M 470.4-6 chg 1, table I-3, *Technical Criteria for Retained Waste*, and have been removed from the processing MBAs. Such materials are referred to as retained waste. Reductions in safeguards for retained waste require the approval of the DOE CSA. The reduced requirements for retained waste materials are:

- Physical protection of retained waste must be commensurate with the safeguards category of the material as defined in DOE M 470.4-6 chg 1, table I-4. Protection measures against other risks, such as radiological sabotage, PP, and information security, may still be required based on results of VAs.
- Nuclear materials accountability information must remain on the site's inventory records and within NMMSS.
- Physical inventory requirements including inventory measurement requirements for material identified in DOE M 470.4-6 chg 1, table I-3 can be deferred until the material is removed from the site; or the material is reintroduced into the processing MBA.

p. Describe the policies and procedures for decommissioning, closure, or deactivation of facilities where MBAs have been established.

The following is taken from DOE M 470.4-6 chg 1.

Identification of a facility (building or other location where an MBA has been established) for decommissioning, closure, or deactivation does not exempt the facility from compliance with requirements stated in DOE M 470.4-6 chg 1. The facility's MC&A program must be maintained at a level commensurate with the category and attractiveness of the nuclear material on inventory until a termination survey determines that no nuclear material remains at the facility. Such a determination may be made if no material remains or the only remaining material is waste or residual holdup that meets the definition of attractiveness level

E and has been written off the MC&A books to a waste management organization. Writing the material off the books means terminating safeguards on the material. With the approval of the DOE CSA, attractiveness level E waste and residual holdup for a facility undergoing decommissioning may be written off the MC&A books to a decontamination and decommissioning organization rather than a waste management organization.

Before a facility is decommissioned, the following must be accomplished.

- All nuclear material holdups must be measured and credited to the accountability books. (After holdup has been measured and properly credited to the accountability books, it can subsequently be written off the books pursuant to DOE M 470.4-6 chg 1, paragraph 1q.) Unless demonstrated to be otherwise, the category of SNM in process holdup must be considered to be the highest category of the total SNM put into the process during its lifetime.
- All nuclear material, except attractiveness level E residual holdup and waste must be transferred to another facility, and the nuclear materials accounting inventory balance must be verified to be zero.
- The termination survey must be completed.

Site/facility operators with decommissioned facilities may still need to maintain a RIS account with NMMSS. For such facilities, transfers of nuclear material in waste to and from other RIS accounts will need to be reported to NMMSS using DOE/NRC F 741/741A, *Nuclear Material Transaction Report*.

With the approval of the DOE CSA, attractiveness level E waste and residual holdup for a facility undergoing decommissioning may be written off the MC&A books to a decontamination and decommissioning organization rather than a waste management organization.

q. Describe the graded safeguards program for the control and accountability for the types and quantities of SNM that can be most effectively used in a nuclear explosive device.

The following is taken from DOE M 470.4-6 chg 1.

The site/facility operator must establish and follow a graded safeguards program for nuclear materials. Under the graded safeguards concept, a safeguards program must provide the greatest relative amount of control and accountability for the types and quantities of SNM that can be most effectively used in a nuclear explosive device. Table I-4 and the following paragraphs present basic information and requirements for determining nuclear safeguards categories.

Categories and attractiveness of nuclear material for implementation of DOE's graded safeguards program are shown in table I-4. Changes to facility safeguards categories that affect protection strategies must be reviewed and approved by the DOE CSA based on materials holdings at the facility and the credibility of rollup.

The material category of SNM locations (e.g., MBAs, MAA, PA, and facilities) must be determined to establish the required protection levels. In many cases, the material category is determined directly from table I-4. Directions for determining the material category when multiple material types and attractiveness levels must be considered are provided in the following paragraphs. Determination of category involves grouping materials by type, attractiveness level, and quantity. Material quantities are element weights for plutonium and isotope weights for uranium-235 (U-235) and uranium-233 (U-233). For the purposes of category determination, quantities of plutonium Material Type 40 and Material Type 50 should be combined and considered as one material type.

- One Material Type, One Attractiveness Level. Sum the material in the attractiveness level and determine the category from table I-4.
- One Material Type, Multiple Attractiveness Levels (where a category III or greater quantity of B-level material is included).
    - Determine the amounts of SNM for materials in each of attractiveness levels B, C, and D.
    - Calculate the "effective" quantity for attractiveness levels B and C by multiplying the quantity in attractiveness levels B and C by the appropriate factors in table I-5, Effective Quantities.
    - Sum the effective amounts in attractiveness levels B and C.
    - Compare the total effective amount, as calculated in DOE M 470.4-6 chg 1, paragraph 2b(2)(c), to the amounts in attractiveness level B from table I-4.
    - Compare the amount of attractiveness level D to table I-4.
    - The material category is the highest level of material category determined using the procedures in paragraphs 2b(2)(a) through 2b(2)(d) or in paragraph 2b(2)(e).
- One Material Type, Multiple Attractiveness Levels (where less than a category III quantity of B-level material is included).
    - Determine the amounts of SNM for all attractiveness levels.
    - Compare the total amounts in each level to those in table I-4.
    - The material category level is the highest level of the material categories determined using the procedures in paragraphs 2b(3)(a) and 2b(3)(b).
- Multiple Material Types.
    - Determine the category for each material type following the above procedures.
    - The category is that determined for the individual material type that requires the highest level of protection.

Roll-up is the accumulation of smaller quantities of SNM to a higher category, based upon a compliance standard using table I-4. Unless it has been demonstrated by a VA that roll-up is not credible, SNM must be safeguarded and protected based on the total quantity of SNM for a location (e.g., MAA, PA, building, or group of buildings).

r. Discuss the MC&A requirements for source and other nuclear materials.

The following is taken from DOE M 470.4-6 chg 1.

Separated neptunium-237 and separated americium (Am-241 and Am-243) must be protected, controlled, and accounted for as if they were SNM. Separated neptunium-237 and separated americium refer to the recovered or product material generated from chemical and processing operations on the target/source material.

- Departmental protection program strategies and graded safeguards thresholds for separated neptunium-237 and separated americium are to be identical to those for U-235. The category for these isotopes is determined using the U-235 side of table I-4.
- Americium and neptunium-237 contained in plutonium as part of the natural in-growth process are not required to be controlled, accounted for, or reported until separated from the plutonium.

Tritium is a nuclear material of strategic importance; therefore, a graded safeguards program for tritium must be implemented according to the following categorizations:

- Category III. Weapons or test components containing reportable quantities of tritium, deuterium-tritium mixtures, or metal tritides that can be easily decomposed to tritium gas, containing greater than 50 grams of tritium (isotope) with a tritium isotopic fraction of 20 percent or greater.
- Category IV. All other reportable quantities, isotopic fractions, types, and forms of tritium.

Excluding tritium, separated neptunium-237, and separated americium (Am-241 and Am-243), source and other nuclear materials listed in table I-1, Nuclear Materials, are exempt from the requirements of this manual except for the following:

- An MC&A program must be established and maintained for these materials based on the strategic and monetary value of the materials.
- Data fields used in the materials accounting system must be consistent with table I-1.
- Nuclear materials inventories and transactions must be documented in the nuclear materials accounting at a level specified by the DOE CSA. At a minimum, all RIS-level inventories and transactions must be documented by the system.
- RIS level transactions and inventories must be reported to NMMSS according to DOE M 470.4-6 chg 1, section B. Transactions and inventories for berkelium are excluded from this requirement and do not need to be reported to NMMSS; however, accounting for berkelium will be maintained at the facility level.
- When these materials are potential substitution materials for SNM and are collocated with SNM, the requirements of DOE M 470.4-6 chg 1, section A, II, 3.a.(2), *Physical Inventory Frequencies*, apply.
- The frequency and manner of conducting physical inventories must be approved by the DOE CSA and documented in the site/facility MC&A plan.
- Other MC&A requirements are to be determined by the DOE CSA and documented in the site/facility MC&A plan or other MC&A program documents.

s. Describe the policies and procedures required in loss detection evaluation, performance testing, and performance requirements.

The following is taken from DOE M 470.4-6 chg 1.

Loss Detection Evaluation

An assessment program for identifying and evaluating facility capability to detect the loss of category I quantities of SNM must be developed for each category I facility. Potential targets must include all category I and any other areas for which a credible scenario for unauthorized accumulation of a category I quantity of SNM has been identified. VAs must be approved by the DOE CSA and must be reviewed annually (at least every twelve months) and updated when there are system changes or new information indicates a potentially significant change in the risk of unauthorized removal of SNM. Results of the reviews, including changes in the VAs, must be reflected in the vulnerability analyses reports. (See DOE M 470.4-1 chg 1 for additional information on VA programs.)

Performance Testing

MC&A performance-testing programs must be developed and documented to support and verify loss detection capability and system effectiveness. (See DOE M 470.4-1 chg 1 for additional information on performance-testing programs.) The scope and intent of performance testing must be based on the graded safeguards concept, (i.e., the testing program demonstrates greater testing for higher category facilities than for lower category facilities), with category I defined as highest and category IV as lowest.

Performance tests must be designed to demonstrate that the MC&A system is functional and to ensure that the system performs as specified or required. In addition, the site/facility operator for the facilities must:

- identify those system components that provide the greatest effectiveness against theft and diversion;
- design, conduct, and document tests that substantiate component effectiveness; and
- integrate the results of these component tests into S&S risk management programs and VAs.

The performance-testing program must include those elements that can detect a threat in time to prevent it and those elements that can effectively account for SNM to detect material loss and ensure that S&S systems are functioning properly. The performance-testing program design must also focus on testing individual detection elements. Elements identified in a VA that contribute to detection capability must be tested on a frequency that is based on the level of risk.

Performance testing must include testing to determine whether S&S systems have failed, including testing for loss of SNM. The accuracy of the accounting system and its capability to provide information about the quantity, location, and identifying characteristics of nuclear material, must be tested.

Corrective action plans for systems that have failed performance testing must be developed and interim compensatory measures put in place.

Performance Requirements

Specific performance requirements for selected MC&A system elements are established below. The performance of the selected system elements must be validated on a frequency documented in the MC&A plan. If system elements fail to meet the performance requirements, a corrective action plan must be developed and, where necessary, compensatory measures must be taken.

- Access Controls. Performance tests must be designed and conducted to evaluate the effectiveness of access controls for category I and II quantities of SNM.
  - At least 95 percent of the tests conducted must demonstrate detection of unauthorized access to category I and II quantities of SNM.
  - Testing of access controls must be facility-specific, and the scope and the extent of the testing must be documented by the site/facility operator and approved by the DOE CSA.
- Material Surveillance. Performance tests must be designed and conducted to evaluate the effectiveness of material surveillance activities for category I and II quantities of SNM.
  - At least 95 percent of the tests conducted must demonstrate detection of unauthorized actions related to the control of category I and II quantities of SNM.
  - Material surveillance testing must be facility-specific, and the scope and the extent of the testing must be documented by the site/facility operator and approved by the DOE CSA.
- The TID record system must accurately reflect the location and identity of TIDs for at least 99 percent of the TIDs inspected. The TID program must ensure that TIDs are properly in place for at least 95 percent of the TIDs inspected.
  - To comply with the TID performance requirement, TIDs must be inspected for all items selected for physical inventory and/or transfer.
  - Testing to ensure TIDs are properly in place must include checking to see that the TID has been properly applied and the integrity of the TID has not been violated.
  - Performance must be verified at least annually (at least every twelve months) except for facilities whose physical inventories are conducted less frequently than once a year. For such facilities, performance must be verified at the same frequency as inventories are conducted.
  - Testing for this requirement is not intended to require destruction of properly applied TIDs whose integrity has not been violated.
- SNM and Metal Portal Monitoring. Performance testing requirements must include those necessary to verify VAs, detection requirements, and applicable tests described in American Society for Testing and Materials (ASTM) International Standard Guides.
- Accounting Record Systems. The accounting record system must accurately reflect item identity and location for at least 99 percent of items selected. If more than 1 percent of the accounting records selected is found to be in error, corrective actions must be taken for the accounting system as a whole.

- Accounting record systems must be verified against all items selected for physical inventory and/or transfer.
- Performance must be verified at least annually (at least every twelve months) except for facilities whose physical inventories are conducted less frequently than once a year. For such facilities, performance must be verified at the same frequency as inventories are conducted.

- For category I and II items, acceptance/rejection criteria for verification measurements and, where possible, for confirmatory measurements, must be based on the standard deviation for the measurement method under operating conditions. Control limits for such criteria must be set at no wider than three times the standard deviation for the method. The control limits must be reviewed and approved by the DOE CSA.
- Inventory Difference Control Limits.
  - For category I and II MBAs, limits-of-error must not exceed 2 percent of the active inventory during the inventory period or a category II quantity of material.
  - For category III and IV MBAs, limits-of-error of inventory differences must not exceed a specified percentage of the active inventory during the inventory period to a maximum of a specified quantity; the specified percentage and maximum quantity must be approved by the DOE CSA.
  - For purposes of the performances requirements, the term "active inventory" means the sum of additions to inventory, beginning inventory, ending inventory, inventory adjustments, and removals from inventory after all "common terms" have been excluded (in this context, "common terms" are material values that appear in the active inventory calculation more than once and come from the same measurement).

t. Describe the policies and procedures required in reporting incidents of security concern.

The following is taken from DOE M 470.4-6 chg 1.

The site/facility operator must identify MC&A loss detection elements for each MBA and must establish a graded program for monitoring these elements and associated data to determine the status of nuclear material inventories and to identify security incidents.

In addition, the DOE CSA must independently evaluate the significance of the incident. Information and actions related to loss detection, monitoring, and assessment activities must be documented and maintained.

The following is taken from DOE M 470.4-1 chg 1.

There may be instances where security incidents are required to be reported through other department reporting systems (e.g., Computer Incident Advisory Capability, Occurrence Reporting and Processing System).

- Any person who observes, finds, or has knowledge or information about a potential incident of security concern must immediately report this information to the FSO or designee of the facility where the incident occurred. The FSO or designee must make notification as specified in DOE M 470.4-1 chg 1, chapter I, paragraph 3.
- Any person discovering a potential incident of security concern, including one that involves classified information or matter; SNM; including material protected, controlled, and accounted for as SNM, or other security interests at risk, must make reasonable efforts to safeguard the security interests in an appropriate manner. The individual must also ensure evidence associated with the incident is not tampered with or destroyed.
- Any person discovering actual or suspected fraud, waste, or abuse of government resources must ensure such incidents are reported to the IG according to DOE O 221.1A.
- Locally developed procedures must be established, documented, approved by the departmental element, and disseminated to ensure the identification, reporting, root cause analysis, and resolution of incidents of security concern. These procedures must also identify guidelines for corrective actions and documentation of time and funds expended on incidents.
- Inquiries must be conducted to establish the facts and circumstances surrounding an incident of security concern.
- Appropriate Federal (to include the Office of Security), state, and local organizations must be contacted when a violation of law is suspected or discovered.
- Appropriate corrective actions must be taken for each incident of security concern to reduce the likelihood of recurrence of the incident, including review and/or revision of applicable S&S plans and procedures.
- The party or parties responsible for an incident of security concern must be subject to appropriate administrative actions, including disciplinary measures, retraining, counseling, or other directed actions necessary to reduce the likelihood of recurrence of the incident.
- Any disciplinary or adverse actions involving DOE employees must be conducted according to DOE Order 3750.1 chg 6.

u. Describe the program to periodically review and assess the integrity and quality of its MC&A program and practice for normal operations and emergency conditions.

The following is taken from DOE M 470.4-6 chg 1.

The site/facility operator must establish a program to periodically review and assess the integrity and quality of its MC&A program and practices. The assessment program must address both normal operations and emergency conditions. The frequency and content of these assessments must be on a graded basis approved by the DOE CSA. (See DOE M 470.4-1 chg 1 for additional information on S&S assessment programs.) The results of all assessments must be reported to the DOE CSA, and assessment reports must be reviewed for classification. Deficiencies must be identified and corrective action plans developed. The assessment must be performed by personnel who are knowledgeable of MC&A.

Reviews must be conducted and documented before startup of new facilities or operations and when changes occur in facilities, operations, or MC&A features that might alter the performance of the MC&A system.

At a minimum, the assessment program must address the following:

- Identification of abnormal situations
- Loss mechanisms, loss detection capabilities, and localization of inventory differences
- Selection, maintenance, calibration, and testing functions to ensure proper equipment and system performance
- MC&A system checks and balances, including separation of responsibilities and duties, used to identify irregularities and detect tampering with materials or MC&A system components
- Change controls, including authorization requirements, to detect unauthorized or inappropriate modification of system components, procedures, or data
- Procedures or checks to ensure the reliability and accuracy of MC&A data and information
- Performance testing conducted by the site/facility operator: this portion of the assessment should address the design of PTs and the results obtained by the testing program since the last assessment
- Procedures for emergency conditions and for periods when MC&A system components are inoperative
- Material containment, MA, and material surveillance procedures
- Physical inventory program and reconciliation practices
- Accounting system procedures, capabilities, and sensitivities
- Identification of personnel with MC&A responsibilities who should be included in the facility HRP
- Measurement control program
- TID programs

In addition to the assessments described above, an organization independent of MC&A must conduct internal audits of the facility's MC&A function to assess compliance with internal plans and procedures. The frequency of these audits must be approved by the DOE CSA.

54. Safeguards and security personnel with the responsibility for MC&A must demonstrate a working level knowledge of the methods for materials accountability.

a. Discuss the accounting system for tracking nuclear material inventories, documenting nuclear material transactions, issuing periodic reports, and assisting with the detection of unauthorized system access, data, falsification, and material gains or losses.

The following is taken from DOE M 470.4-6 chg 1.

A system for tracking nuclear material inventories, documenting nuclear material transactions, issuing periodic reports, and assisting with the detection of unauthorized system access, data falsification, and material gains or losses must be established and implemented. The accounting system must provide a complete audit trail for all nuclear material from receipt through disposition. The generally accepted accounting principles promulgated by the Financial Accounting Standards Board must be used in the design and operation of the nuclear material accounting system.

The facility nuclear materials accounting system must include checks and balances and must be structured to ensure timely detection of errors or discrepancies in records associated with a category I or II quantity of SNM, including, where possible, detecting falsified data and identifying the responsible persons. Timeframes for detection of errors and discrepancies must be approved by the DOE CSA and documented in the MC&A plan. The system also must be capable of detecting omissions and other data discrepancies and ensuring completeness of accounting records.

Procedures must be established and maintained that describe the structure and operation of the nuclear materials accounting system. The procedures must accurately reflect current nuclear material accounting practices. Specific requirements for accounting procedures must include the following.

- Descriptions of the inventory database (including procedures for updating and reconciling inventory data with the results of physical inventories) and the required data elements for each applicable material type
- Identification of accounting reports and their frequency, distribution, and timeliness, consistent with accounting requirements
- Identification of organizational responsibilities for management and operation of the accounting system
- Recording, reporting, and submitting data to the NMMSS, by material type and reporting unit, as specified in DOE M 470.4-6 chg 1, section B

Account Structure.

- Facility nuclear material accounts must consist of one or more MBAs established to identify the location and quantity of nuclear materials in the facility. Readily retrievable accountability data must be maintained by the MBA and reflect quantities of nuclear materials inventory, quantities of nuclear materials received and shipped, and other adjustments to inventory.
- The MBA account structure must sort data by material types, processes, and functions; provide the capability to localize inventory differences; and provide a system of checks and balances for verifying the accuracy of the accountability data and records.
- An MBA boundary must not cross another MAA boundary. Each MBA must consist of a single geographical area and be an integral operation.
- The site/facility operator must designate an MBA custodian for each MBA to ensure that MC&A requirements are implemented in that MBA.

- The MBA custodian is responsible for controlling nuclear material located in the MBA, preparing and signing internal material transfer documents, and conducting and reconciling MBA physical inventories.
- An MBA custodian must not be responsible for multiple MBAs when transfers of nuclear material occur between those MBAs (i.e., a single custodian must not serve as both shipper and receiver for material transfers).

The site/facility operator must maintain records, submit data, and issue reports as required by DOE M 470.4-6 chg 1 and facility procedures. The reports must accurately describe all nuclear materials transactions and inventories. Inventory adjustments must be identified by the MBA and must be reported as required in DOE M 470.4-6 chg 1.

Nuclear materials records must be updated by authorized personnel only. The records system must provide an audit trail for all transactions affecting the nuclear materials database.

The accounting records system must be capable of being updated daily or on demand for all nuclear materials transactions. This requirement is for updating records based on reports or information; it does not pertain to how quickly a facility must be able to complete measurements. The records system must also be capable of generating electronic and/or hard copy book inventory listings of all SNM within three hours. The listing must differentiate between SNM and other nuclear material when necessary. The accuracy of the accounting record system must be validated in accordance with requirements of DOE M 470.4-6 chg 1, section A, chapter I, paragraph 4b. Specific performance requirements for accounting record system accuracy are contained in DOE M 470.4-6 chg 1, chapter I, paragraph 4c.

b. Describe the physical inventory program for nuclear materials to demonstrate that materials are present in their stated quantities and to detect the unauthorized removal of nuclear materials.

The following is taken from DOE M 470.4-6 chg 1.

The site/facility operator must implement a physical inventory program for nuclear materials to demonstrate that materials are present in their stated quantities and to detect the unauthorized removal of nuclear materials. Inventory requirements for separated neptunium and separated americium are the same as for SNM. When facilities are precluded from performing physical inventories as required by DOE M 470.4-6 chg 1, material control and protection features must be enhanced to ensure inventory integrity. Physical inventory programs must comply with the following requirements:

- Periodic and special physical inventories must be performed for each MBA according to the strategic importance of the material and the consequence of its loss.
- Inventories must be based on measured values, including measurements or technically justifiable estimates of holdup. Process monitoring techniques may be used for material that is undergoing processing and recovery operations and is inaccessible for measurements. Plans and procedures must be developed and documented that define responsibilities for performing inventories and specify criteria

for conducting, verifying, and reconciling inventories. Statistical sampling, based on graded safeguards, may be used to verify the presence of items during inventories. Parameters for statistical sampling plans must be defined by the site/facility operator, and approved by the DOE CSA. Sampling plans must specify the population, confidence level, minimum detectable defect, definition of a defect, and action to be taken if a defect is encountered.

- Physical inventories must be performed for category I and II MBAs that involve activities other than processing at a frequency determined by the DOE CSA but at least semiannually (once every six months). The site/facility operator must ensure that physical inventories are performed bimonthly (once every two months) in category I and II MBAs where processing occurs.
- Extensions to inventory frequencies must be approved by the DOE CSA in accordance with the alternative inventory control provisions in DOE M 470.4-6 chg 1, table II-2, *Inventory Periods Based on Alternative Measures for Category I and II Storage Locations*. For category I and II storage areas, table II-2 may be used to determine the frequency of physical inventories based on the successful implementation of alternative inventory control measures. Inventory periods specified for each alternative measure are additive so long as the measures function independently.
- A physical inventory reconciliation program must be implemented in which the book inventory for each MBA is compared with, and if necessary, adjusted to the physical inventory. The reconciliation must be completed within fifteen calendar days following receipt of all inventory information, measurement data, and sample analyses. Any inventory differences must be identified and reported as required.
- Procedures must be established and implemented for conducting special inventories at the request of authorized facility personnel, the DOE CSA, or as a result of routine disassembly of critical assemblies, changes in custodial responsibilities, missing items, inventory differences exceeding established control limits, and abnormal occurrences.
- A system for performing measurements as part of a physical inventory must be established and implemented by the site/facility operator for each MBA. Verification measurements must be made on SNM items that are not tamper-indicating. Verification measurements must also be made on tamper-indicating items that are not under an effective materials surveillance program.

c. Describe the Measurement and Measurement Control Programs used to determine Category I or II inventories of SNM.

The following is taken from DOE M 470.4-6 chg 1.

Measurement and measurement control programs approved by the DOE CSA must be implemented at all facilities with nuclear material. Measurement programs used to determine category I or II inventories of SNM or used to determine a category I or II SNM throughput over a 6-month period must meet the requirements set forth in DOE M 470.4-6 chg 1, section A., chapter II, paragraphs 4a-4e. All measurement systems used for accountability purposes

must have associated measurement control programs to ensure the quality of measurement data generated.

Measurement programs used to determine category III or IV inventories of SNM must address the topics set forth in DOE M 470.4-6 chg 1, paragraphs 4a-4e, below, but the specific measurement and measurement control requirements will be determined by the DOE CSA.

Measurement systems used for accountability purposes must be precise and accurate enough to minimize the contribution of measurement error to the limit of error of the inventory difference. Nuclear materials not amenable to verification measurement must be identified in the facility's MC&A plan. Inventory values for these materials must be based on measured values or technically justified estimates. Justification and supporting documentation for these inventory values must be maintained and readily retrievable for review.

- Organization. Measurement and measurement control programs must be independent from operations.
- Selection and Qualification of Measurement Methods. The site/facility operator must select, qualify, and validate measurement methods capable of providing the required levels of precision and accuracy. Target values for precision and accuracy of nuclear material measurements endorsed by recognized national and international nuclear organizations must be considered performance goals for facility measurement systems. Alternative measurement performance goals must be defensible and documented. Precision and accuracy requirements must be approved by the DOE CSA and documented in the MC&A plan. Procedures must be documented and implemented for each facility to ensure that only qualified measurement methods are used for accountability purposes.
- Training and Qualification of Measurement Personnel. Individuals responsible for performing nuclear material measurements must have sufficient knowledge to perform the measurements in an acceptable manner.
    - Training. A documented plan for training measurement personnel must be established and implemented for each facility. The plan must be reviewed annually (at least every twelve months) and updated as necessary to reflect changes in measurement technology and must specify training qualification and re-qualification requirements for each measurement method.
    - Qualification. A documented qualification program must be established and implemented for each facility to ensure that measurement personnel demonstrate acceptable levels of proficiency before performing measurements and that measurement personnel are re-qualified according to requirements in the training plan. Measurement personnel must demonstrate proficiency in destructive analysis of nuclear material at a minimum of once per day for each method they will use that day.

Nuclear material measurement systems must provide accurate nuclear material values for inventories and transactions.

- Sampling. Sampling programs must be implemented to ensure that portions of bulk material taken for measurement are representative of the bulk material. The site/facility operator must establish and implement a documented sampling plan for each measurement point used for accountability purposes. The plans must be based on valid technical and statistical principles and must take into account material type, measurement requirements, and any special process or operational considerations.
    - The basis for the sampling plan must be documented and validated through studies of the materials or items being sampled.
    - The sampling plan must specify, at a minimum, the sampling procedure, number and size of required samples, mixing time and procedure (when applicable), provisions for retaining archive samples, and estimates of variance associated with the sampling method.
    - Sampling procedures must be documented and reviewed annually (at least every twelve months) or whenever changes are made, including changes to the type or composition of the material being sampled.

The site/facility operator must develop, document, and maintain measurement methods for all nuclear material on inventory. These methods must be written to provide clear direction to the analyst or operator and must be validated initially and revalidated whenever changes are made.

- In determining inventory values and consistent with the graded safeguards concept, measurement methods must be selected in a manner that minimizes the contribution of measurement error to the uncertainty of the inventory difference.
- Verification measurements, when used to adjust accountability records, must have accuracy and precision comparable to, or better than the original measurement method.
- The method used for confirmatory measurements must be capable of determining the presence or absence of a specific attribute of the material consistent with valid acceptance and rejection criteria.
- All measurement methods must be calibrated using standard or certified reference materials or secondary standards traceable to the national measurement base and must be revalidated as necessary.
- Measurement equipment and instruments must meet precision and accuracy requirements under in-plant conditions.
- Documentation of measurement data must be maintained to provide an audit trail from source data to accounting records.

The site/facility operator must develop and implement control programs for all measurement systems used for accountability purposes. Control programs must ensure the effectiveness of measurement systems and the quality of measured values used for accountability purposes. Control programs must also produce precision and accuracy values for use in determining inventory difference control limits and shipper/receiver limits of error. A measurement control program, as referred to herein, must include, at a minimum, the following elements.

- Scales and Balances Program. All scales and balances used for accountability purposes must be maintained in good working condition, recalibrated according to an

established schedule, and checked for accuracy and linearity on each day that the scale or balance is used for accountability purposes.

- Analytical Quality Control. Data from routine measurements must be analyzed statistically to determine and ensure accuracy and precision of the measurements.
- Sampling Variability. The uncertainty associated with each sampling method, or combination of sampling and measurement methods, must be determined and maintained on a current basis.
- Physical Measurement Control. The precision and accuracy of volume, temperature, pressure, and density measurements must be determined and ensured.
- Instrument Calibration. Instruments must be calibrated using appropriate standards, when available. At a minimum, measurement values must be compared with more accurate measurement system values on a prescribed basis; the frequency is defined by demonstrated instrument performance.
- Reference Materials (Standards). All calibration and working standards used in a measurement control program must be traceable to the national measurement base through the use of standard reference materials or certified reference materials. They must have smaller uncertainties associated with their reference values than the uncertainties of the measurement method in which they are used. Working standards used in a measurement control program must be representative of the type and composition of the material being measured when the material matrix affects the measured values.
- Sample Exchange Programs. Each facility's measurement control program must include participation in inter-laboratory control programs to provide independent verification of internal analytical quality control.
- Statistical Controls. For each measurement method used for accountability purposes, control limits must be calculated and monitored, and documented procedures must exist to correct out-of-limits conditions. Control limits must be established at the two-Sigma level (warning limits) and three-Sigma level (alarm limits). Control data exceeding the two-Sigma limits must be investigated, and when warranted, corrective action must be taken. If a single data point exceeds the three-Sigma level, the measurement system in question must not be used for an accountability measurement until the measurement system has been demonstrated to be within statistical control. For measurement methods relying substantially on operator technique, control limits must include uncertainties for each analyst/method combination. Statistical control limits must be monitored to ensure they are consistent with target values as approved in the MC&A plan.
- Measurement Method Qualification. The site/facility operator must have a documented measurement method qualification program. The qualified measurement methods must demonstrate acceptable performance before being used for accountability purposes. For destructive analysis and nondestructive assay of nuclear material, performance must be demonstrated at least once per day for each method being used. For nondestructive analysis measurement systems for which meeting this requirement is impractical or unnecessary, the control measurement frequency must

be at least one of every five measurements unless otherwise approved by the DOE CSA.

- Measurement Control Procedures. The site/facility operator must develop and document measurement control procedures for all measurement methods used for accountability. The site/facility operator must develop and implement a program for each facility to ensure measurement control procedures are followed.
- Statistical Programs. The site/facility operator must develop and implement a documented program for the statistical evaluation of measurement data to determine control limits and precision and accuracy levels for each measurement system used for accountability. The program must ensure the quality of measurement and measurement control data and provide estimates of uncertainty on inventory and inventory control statements. The statistical program, at a minimum, must contain the following elements:
  - Valid statistical techniques to determine the total random error, the measurement biases generated for each measurement system or sampling/measurement system, and the control limits, rejection limits, and outlier criteria.
  - A valid statistical technique to develop sampling plans for inventory and measurement of nuclear material.
  - Analysis of measurement control data and reporting to the responsible organization at specified times and frequencies.
  - Documentation of all major assumptions made in each data evaluation process.

d. Discuss the Nuclear Material Transfers Program used to control and account for both internal and external transfers of nuclear materials for each facility. Define the procedures that specify requirements for authorization, documentation, tracking, verification, and response to abnormal situations that may occur during transfer of nuclear materials.

The following is taken from DOE M 470.4-6 chg 1.

The site/facility operator must develop and implement a program to control and account for both internal and external transfers of nuclear materials for each facility. This program must include documented procedures that specify requirements for authorization, documentation, tracking, verification, and response to abnormal situations that may occur during transfer of nuclear materials. The site/facility operator must establish and implement a graded system of measurements and records to monitor internal and external transfers of nuclear material and to deter/detect unauthorized removal of material during such transfers (see DOE M 470.4-6 chg 1, section B for requirements for submitting DOE/NRC F 741 and DOE forms required for documenting transfers for materials accounting purposes).

e. Describe the graded system of measurements and records that monitors internal and external transfers of nuclear material to deter/detect unauthorized removal of material during such transfers.

The following is taken from DOE M 470.4-6 chg 1.

Internal Transfers

The site/facility operator must provide a graded system of measurements and records to reflect the flow of material between MBAs within that facility and between it and other facilities on the same site. The facility control system must be designed to monitor transfer activities and to deter and detect unauthorized removal of material during transfers. It must flag abnormal situations.

Transfers must be documented on nuclear material transfer forms or electronic equivalents that contain required information, prepared and distributed within established time frames, and signed by authorized custodians or their alternates. Materials must be subjected to a transfer check within one work day after receipt to include verification of shipping containers or item count, TID integrity, and identification number. When the isotope content of SNM transferred between MBAs is 50 grams (fissile) or more, the material must have a measured value before transfer.

Acceptance/rejection criteria must be established and documented to evaluate measurement data for internal material transfers. In addition, procedures must specify notification and response requirements if nuclear material removal or another abnormal situation is detected.

External Transfers

The shipper must obtain written verification and maintain documentation that the intended receiver is authorized to accept the material before the material is transferred.

Transfers of nuclear material between facilities having a different RIS must be documented using the electronic equivalent of DOE/NRC F 741. These forms must be prepared and distributed to the principals of the transaction and line management.

Immediately after receipt, shipments must be subjected to a transfer check. Records of transfer checks are subject to audit and must be retained at least until the next S&S survey. For accountability purposes, material in transit at the end of a reporting period must be included in the receiver's reported inventory even though physical receipt of the material has not yet occurred.

For all unirradiated category I and II quantities of SNM transferred between facilities having a different RIS, the receiver must perform a verification or accountability measurement unless both RISs are located on the same site and are operated by the same site contractor. Accountability measurements are entered in the receiver's accountability system as the value for the shipment.

The shipper must independently determine the measured values before shipment unless the integrity of the item and of the existing measured values have been ensured. The shipper's measured values must be documented on DOE/NRC F 741.

f. Describe the Material Control Indicators Program for detecting losses through evaluation and assessment of shipper/receiver differences, inventory differences, and other inventory adjustments.

The following is taken from DOE M 470.4-6 chg 1.

The site/facility operator must develop and implement a program that is capable of detecting losses through evaluation and assessment of shipper/receiver differences, inventory differences, and other inventory adjustments. The program must assess the material control indicators described below and ensure detection of losses and unauthorized removal of nuclear materials. Documented plans must specify responsibilities and procedures for evaluating material control indicators.

Written procedures must be developed for evaluating shipper/receiver differences and for investigating and reporting significant shipper/receiver differences. A shipper/receiver difference is defined to be significant when it meets any of the following criteria:

- It involves a discrepancy in the number of items, regardless of the quantity of nuclear material, or confirmation measurements for the shipment fail to meet acceptance criteria covered in a shipper/receiver agreement.
- It is statistically significant. The determination of whether shipper/receiver difference is statistically significant is only required for those shipments for which verification/accountability measurements are made by both the shipper and receiver. A shipper/receiver difference is defined to be statistically significant when the magnitude of the difference exceeds either:
  - the limit obtained by a statistical combination of the valid limits of error for the shipper and receiver's measured values; or
  - the square root of two times a single valid limit of error when either the shipper or receiver's limit of error is invalid. When both the shipper's and receiver's limits of error are determined to be invalid, the limits of error must be recalculated, and the statistical significance of the shipper/receiver difference must be reevaluated.
- Shipper/receiver difference data must be subjected to trend analysis to detect measurement bias or material loss. Analyses must be designed to detect statistically significant cumulative shipper/receiver differences and to trigger investigations when these differences are detected.
- The receiver must notify its DOE CSA and the shipper of any shipper/receiver difference determined to be significant. Both shipper and receiver must investigate their measurements and limits of error. Such investigations must be completed and documented.
- Shipper/receiver differences involving a discrepancy in number of items must be reported.
- When shipper/receiver differences are determined to be statistically significant, but the quantities and strategic or monetary values are insufficient to warrant an investigation and subsequent correction to transfer documents, and when the receiver is DOE or one of its contractors or subcontractors, the difference need not be

investigated and the party must record its own quantitative value. In the context of this paragraph, differences of less than 50 grams of fissile material or less than 5 grams of tritium are considered to be insufficient to require an investigation unless there are special circumstances. Authority to invoke the stipulations of this paragraph rests mutually with the shipper's and receiver's DOE CSA.

- Statistically significant shipper/receiver differences may be resolved through any of the following methods:
  - If both the shipper's and receiver's DOE CSA obtain assurance that the measurements and limits of error are valid, and the investigation indicates that theft or diversion has not occurred, the shipper and receiver must record their own quantitative values.
  - If either the shipper or receiver and their DOE CSA agree to accept the other's value, the shipper or receiver must prepare a corrected copy of the shipping document using the other's data.
  - If the investigation does not result in a satisfactory resolution, the shipper/receiver difference must be resolved by the departmental elements concerned through traditional DOE line management channels.
- The receiving facility must not process SNM contained in a shipment involving an unresolved significant shipper/receiver difference unless a shipper/receiver agreement allowing this has been approved by both the shipper's and receiver's DOE CSA.

55. Safeguards and security personnel with the responsibility for MC&A must demonstrate a working level knowledge of the methods for materials control.

a. Describe the Access Controls Program that controls personnel access to nuclear materials; nuclear material accountability, inventory, and measurement data; data-generating equipment; and other items/equipment the misuse of which could compromise the safeguards system.

The following is taken from DOE M 470.4-6 chg 1.

Personnel Access

A graded program must be established to control personnel access to: nuclear materials; nuclear materials accountability, inventory, and measurement data; data-generating equipment; and other items/equipment the misuse of which could compromise the safeguards system.

Materials Access

A documented program must be established and implemented for each facility to ensure that only properly authorized personnel have access to nuclear materials. This program must address procedures and mechanisms to detect and respond to access by unauthorized personnel. To minimize the potential for unauthorized access to nuclear material, the amount of material in use must be limited to that necessary for operational requirements, and excess

material must be stored in repositories or kept in enclosures designed to ensure that access will be limited to authorized individuals.

Data Access

Procedures must be established that ensure only authorized persons have the ability to enter, change, or access MC&A data and information.

Equipment Access

Access must be controlled to data-generating and other equipment used in material control activities. Such equipment includes measurement equipment, data-recording devices, and TIDs.

Other Considerations

Access control programs must protect against unauthorized data and equipment modification and detect unauthorized activities during emergency or other unusual conditions.

b. Describe the Nuclear Material Surveillance Program used to ensure that nuclear materials are in their authorized locations, detect unauthorized activities or anomalous conditions, and report material status in both normal and emergency conditions.

The following is taken from DOE M 470.4-6 chg 1.

Material surveillance methodologies must include: automated systems (e.g., monitoring devices, sensors, or other instrumentation); or visual surveillance/direct observation (e.g., the two-person rule, monitoring by external personnel); or other alternative safeguards measures that provide the necessary detection. When the direct observation method is used, the observer must have the means to recognize, correctly assess, and report activities that are unauthorized or inconsistent with established S&S requirements.

Surveillance procedures must describe the methodologies and operational/control points on which the program is based and provide for investigation, notification, and reporting of anomalies.

Material surveillance programs for category I and II quantities of SNM must ensure that materials are in authorized locations and that unauthorized material flows and transfers are detected. Category I locations must be evaluated to determine the ability of the material surveillance system to assess material losses from MAA and PA boundaries. Category II locations must be evaluated to determine the ability of the material surveillance system to assess material losses from the PA boundary. Material surveillance programs for all areas containing category I or II quantities of SNM must include the following measures:

- Only authorized and knowledgeable personnel who are capable of detecting incorrect or unauthorized actions can be assigned responsibility for surveillance of SNM.
- Controls must be sufficient to ensure that a lone individual cannot gain access to a secure storage area.

- All persons in secure storage areas must be under constant surveillance (e.g., the two-person rule or equivalent surveillance) at any time the storage area is not locked and protected by an active alarm system.
- Surveillance must ensure that unauthorized or unaccompanied authorized personnel cannot enter the storage/processing area undetected when the door is unlocked or open.
- When items are outside an alarmed storage area within an MAA or PA, there must be a system of hardware, procedures, and administrative controls sufficient to ensure that unauthorized accumulation of a category I quantity is detected. When the two-person rule is utilized as an administrative control, the two authorized persons assigned responsibility for maintaining direct control of the items must be physically located where they have an unobstructed view of each other and the items. SNM in use or process must be under material surveillance, under alarm protection, or, with the approval of the DOE CSA, protected by alternative means that can be demonstrated to provide equivalent protection.
- Material surveillance programs must ensure that attempts to remove SNM from tamper-indicating items without proper authorization will be detected. The effectiveness of the material surveillance program in meeting this requirement must be analyzed and documented.

Category III. The material surveillance program for category III quantities must ensure that when materials are not in locked storage, they are attended, are in authorized locations, and are not accessed by unauthorized persons.

Category IV. Graded site/facility material surveillance programs must be developed and implemented for category IV quantities based on the consequence of their loss. The programs must ensure that the materials are in authorized locations and are not accessed by unauthorized persons.

c. Describe the Material Containment Program that provides controls for nuclear materials operations relative to MAA, PA, MBA, other authorized storage repositories, and processing areas.

The following is taken from DOE M 470.4-6 chg 1.

Controls for Nuclear Materials Operations

A documented program must be in place to provide controls for nuclear materials operations relative to MAAs, PAs, MBAs, other authorized storage repositories, and processing areas.

Controls must be in place to ensure that category I quantities of SNM are used, processed, or stored only within an MAA contained in a PA and that category II quantities of SNM are used, processed, or stored only within a PA. The containment program must do the following:

- Identify authorized activities and locations for nuclear materials
- Identify mechanisms used to detect unauthorized activities

- Identify material types, forms, and amounts authorized to be removed from the MAA or PA
- Identify containment controls for normal and emergency conditions
- Require a periodic audit of the containment program to ensure compliance and system effectiveness
- Evaluate roll-up

Controls must be established and implemented for each facility to ensure that nuclear materials are used, processed, or stored within an MBA and are controlled in accordance with the graded safeguards concept. These controls must ensure that materials are removed only through authorized pathways or portals and are subject to transfer and verification procedures identified in DOE M 470.4-6 chg 1, section A, chapter II, paragraph 5. Controls for MBAs must meet the following:

- Be formally documented
- Identify geographical boundaries and functions of the MBA
- Identify material types, forms, and quantities permitted in each MBA
- Describe administrative controls for each MBA
- Define custodial responsibilities for nuclear materials contained within an MBA
- Identify personnel authorized to receive or ship nuclear material
- identify material flow into and out of the MBA;
- Ensure material transfer procedures are followed
- Ensure that material quantities transferred across MBA boundaries are based on measured values consistent with DOE M 470.4-6 chg 1, chapter II, paragraph 5b(5)

Other Authorized Storage Repositories

This information is taken from DOE M 470.4-2A.

An SNM vault must be a penetration-resistant enclosure that has doors, walls, floor, and roof/ceiling designed and constructed to significantly delay penetration from forced entry and equipped with instruction detection system devices on openings allowing access. The material thickness must be determined by the requirement for forcible entry delay times for the S&S interests stored within, but must not be less than the delay time provided by a minimum 8-inch (20.32-centimenters)-thick reinforced concrete poured in place with a 28-day compressive strength of 2,500 pounds per square inch (17,237 kilopascals). Activated technologies such as activated barriers or passive/active denial systems may be used in lieu of thicker concrete when analysis indicates that delay times exceeding that of 8-inch (20.32-centimeters)-thick reinforced concrete are required. The site's analysis of the protection measures in use must be documented in the SSP.

A vault door and frame must meet the GSA's highest level of penetration resistance. The lock on the door must be a minimum of a GSA-approved Federal supply schedule-listed high-security lock, as described in DOE M 470.4-2A, chapter IV.

Any openings of a size and shape to permit unauthorized entry (larger than 96 square inches [619.2 square centimeters] in area and more than 6 inches [15.24 centimeters] in its smallest

dimension) must be equipped with the measures described in DOE M 470.4-2A, chapter VIII.

Processing Areas

The following is taken from DOE M 470.4-6 chg 1.

Controls must be established for nuclear materials being used or stored in processing areas. The controls for in-process areas must do the following:

- Describe activities and locations for storing material
- Identify components used to detect unauthorized activities or conditions
- Include procedures for moving material into or out of the processing area
- Describe control procedures for normal and emergency conditions and for maintenance activities
- Describe response actions to be taken in abnormal situations
- Provide for audit of the processing controls on a periodic basis to ensure system effectiveness

d. Describe detection/assessments systems that are in place to detect and assess the unauthorized removal of nuclear materials, consistent with the graded safeguards concept.

The following is taken from DOE M 470.4-6 chg 1.

A documented program, administered by the MC&A organization, must be in place to control TIDs and ensure that TIDs are used to detect violations of container integrity. TID programs cannot be regarded as effective unless used in conjunction with a material surveillance program. Testing of TID integrity, location, application, and the TID record system must be conducted. The TID control program must include the following elements:

- ID acquisition/procurement/destruction
- Types of TIDs used
- Unique TID identification
- Storage
- Issuance
- Personnel authorized to apply, remove, and dispose of TIDs
- Containers on which TIDs are to be applied
- Procedures for application of TIDs
- Frequency and method of TID verification
- Procedures for responding to, and reporting of TID violations
- Assurance that TIDs cannot be reused after violation
- Frequency and method of internal program audits
- A DOE CSA approved listing of all containers considered to be intrinsically tamper-indicating

The detection level of the SNM portal monitors must be based on the types and forms of SNM used, stored, or processed in the area and the credible number of removals associated with theft of a

category I quantity of SNM. Controls must be established to prevent unauthorized access to portal monitor instrumentation and cabling. A written response plan must be prepared and implemented to provide evaluation and resolution of all alarm conditions.

Waste Monitors

- All liquid, solid, and gaseous waste streams leaving an MAA must be monitored to detect the theft or diversion of SNM. Facility waste-monitoring equipment must be maintained and controlled to ensure that the equipment is capable of detecting specified amounts of SNM as determined by the DOE CSA. Instrumentation used to monitor waste and equipment removed from an MAA must be able to detect, in combination with other detection elements, the removal of a category I quantity of SNM through a credible theft or diversion scenario.
- A response plan for evaluating and resolving situations involving any discharge exceeding facility-specific limits must be established by the site/facility operator for the facility, and approved by the DOE CSA.

e. Define how the detection/assessment system(s) are interfaced with the facility's physical protection and other organizational systems, as appropriate, and how they detect and localize removal of SNM from its authorized location, and notify the PF and other organizations to respond when such events are detected.

The following is taken from DOE M 470.4-6 chg 1.

Systems must be in place to detect and assess the unauthorized removal of nuclear materials, consistent with the graded safeguards concept. The system must be interfaced with the facility's physical protection and other organizational systems, as appropriate, and must be able to detect and localize removal of SNM from its authorized location, and notify the PF and other organizations to respond when such events are detected.

f. Discuss the detection/assessment of unauthorized removal of nuclear material.

The following is taken from DOE M 470.4-6 chg 1.

MC&A systems must be established for monitoring and control to provide the capability of detecting and assessing unauthorized SNM removals. Systems can include weight sensors, SNM/physical presence detectors, fiber optic seals, surveillance cameras, vault monitors, emergency egress radiation monitors, real-time inventory locator systems, etc. The MC&A system must provide sufficient information to correctly assess the alarms, localize the removal, and estimate the quantity and form of the diverted or stolen material.

Daily administrative checks must be implemented for each category I MBA (or multiple MBAs where roll-up to a category I quantity of SNM is credible). The DOE CSA must determine and approve the scope and extent of the checks and specify the detection objectives on the basis of recognized vulnerabilities.

56. Safeguards and security personnel with the responsibility for MC&A must demonstrate a working level knowledge of the requirements for NMMSS reporting and data submission.

a. Discuss the documentation and reporting requirements for all RIS level nuclear materials transactions, material balances, and inventories into the NMMSS.

The following is taken from DOE M 470.4-6 chg 1.

All RIS-level nuclear materials transactions, material balances, and inventories must be documented in accordance with the instructions provided in DOE M 470.4-6 chg 1, section B and reported to the NMMSS, the national database for nuclear materials.

The NMMSS will be used to accumulate and distribute information concerning nuclear materials transactions, material balances, and inventories.

Submissions must be made in a timely manner to achieve reporting of accurate and complete data as soon as possible after the events described by the data occur.

The national database will provide nuclear materials information relating to safeguards, materials management and production, inventory quantities and valuations, and other information requested or required by DOE and NRC.

The national database will serve as the centralized reporting facility to provide the information required under the provisions of the U.S./IAEA Safeguards Agreement.

All NMMSS data submissions that are mailed will be sent to the NMMSS operator at—

NAC International
NMMSS Project
P.O. Box 922088
Norcross, GA 30010
Attn: Document Control

The correct manuals to use when reporting nuclear material to NMMSS are as follows:

- DOE M 470.4-6 chg 1 will be used to report all U.S. government-owned (owner code G) nuclear materials (see tables XV-1 and XV-3), and non-government owned (owner code J) nuclear materials located on a DOE site.
- NRC Nuclear Regulation (NUREG)-0006, Instructions for Completing Nuclear Material Transaction Reports, and NRC NUREG-0007, Instructions for the Preparation and Distribution of Material Status Reports, are used to report non-government-owned (owner code J) nuclear materials located at a licensee facility.
- Facilities, projects, and programs under the cognizance of the Office of Civilian Radioactive Waste Management subject to NRC regulation must use the rules, standards, and criteria specified by the NRC or the NRC agreement state in lieu of DOE M 470.4-6 chg 1.

b. Describe the data collection forms (or the electronic equivalent) used to document and report nuclear materials transactions, material balances, and inventories.

The following is taken from DOE M 470.4-6 chg 1.

Data collection forms identified and described in DOE M 470.4-6 chg 1, chapter XVII, (or the electronic equivalent) will be used to document and report nuclear materials transactions, material balances, and inventories in accordance with the instructions provided in DOE M 470.4-6 chg 1.

A computer-generated form must contain all information necessary for proper documentation and reporting of nuclear materials transactions, material balances and inventories. Examples of the paper forms are provided in DOE M 470.4-6 chg 1, chapter XVII, for informational purposes and are not to be used to supply data to the NMMSS. The required forms that must be used are available from the NMMSS operator and online at the DOE directives website (www.directives.doe.gov).

c. Discuss the establishment, maintenance, and deactivation of an individual RIS.

The following is taken from DOE M 470.4-6 chg 1.

Establishment of RIS

To establish a new RIS the following procedure applies:

- A request from the MC&A field representative, who may be either a DOE Federal or contractor employee, is routed to the DOE CSA for review and approval.
- A DOE HQ sponsoring program office must approve activities for which the RIS is requested.
- The request is then sent from the DOE CSA, through the appropriate HQ program office, for coordination with the Office of Resource Management to establish the RIS required for DOE approved activities.
- The Office of Resource Management instructs the NMMSS operator to add the RIS.

Justification must exist before a new RIS can be established. The following is a list of common reasons for requesting a new RIS. The facility must

- anticipate departmental authorization to contain an inventory of nuclear materials within the next twelve months;
- be involved in international shipments or receipts of nuclear materials;
- be storing or processing material under atomic energy agency safeguards.

A facility that does not meet the above criteria, but believes a RIS is necessary for operations, can request a RIS by submitting proper justification and documentation through the DOE CSA to the Office of Resource Management by following the procedure outlined in DOE M 470.4-6 chg 1, paragraphs 2a(1) through (4).

Maintenance

The following procedure must be followed to change information entered on a facility's RIS directory page:

- Make a copy of both sides of the page from the RIS directory for each affected RIS.
- Draw a line through the outdated/erroneous information on the copy.
- Immediately above the strike-out, print the new information clearly.
- Submit the pages marked for change to the NMR, or other authorized person who will sign and date all directory pages on which changes have been recorded. Unsigned changes cannot be made.
- Send page changes to the DOE CSA for approval and forwarding to the NMMSS operator.

The NMMSS operator will provide a written copy to the Office of Resource Management for information/file purposes.

Deactivation of RIS

RIS deactivation will occur when a facility's authorization to store/handle nuclear materials inventory is withdrawn. Before deactivation, all open transactions must be resolved and all inventory removed to a balance of zero.

The NMR of the RIS being deactivated should initiate and receive certification from the NMMSS operator that no project numbers exist for that RIS. If there are project numbers associated with the RIS that is to be deactivated, the project numbers must be cancelled or changed to reflect proper status of the material.

An assessment by the MC&A field representative must conclude the following:

- All physical MC&A activities have been terminated.
- All material has been shipped from the facility.
- The balance for that RIS in NMMSS is zero (0).
- No investigations or audits are under way concerning any aspect of MC&A.

Notification of deactivation is sent from the DOE CSA to the Office of Resource Management, who will instruct the NMMSS operator to deactivate the RIS.

A waste facility's RIS must not be removed except with specific approval of the responsible departmental element through the DOE CSA and upon coordination with the Office of Resource Management.

A parent RIS must not be deactivated when a sub-RIS is still active.

57. Safeguards and security personnel with the responsibility for MC&A must demonstrate a working level knowledge of the requirements for nuclear materials transaction reporting.

a. Describe the documentation and reporting of the physical transfer of nuclear material.

The following is taken from DOE M 470.4-6 chg 1.

Data on all transactions occurring during a calendar month will be submitted no later than eight working days following the end of the month during which the transactions occurred. Facilities must distribute transaction documentation electronically unless manual/paper submission is coordinated through the DOE CSA.

Electronic Method

- Procedures and instructions in DOE M 470.4-6 chg 1 will apply except that signatures on transaction documents are not required. Internal controls will ensure that data transmitted has been properly authorized.
- The sender and recipient of electronic data will produce hard copies as needed by organizations on the distribution lists in DOE M 470.4-6 chg 1, table III-2 and table III-3.
- The hard copies will contain the information normally included on DOE/NRC F 741.
- For activities involving NRC or Agreement State licensees, the electronic method of handling and transmitting transfer data will follow all requirements of 10 CFR 74, "Material Control and Accounting of Special Nuclear Material."

Manual Method

- Facilities with a low volume of reporting activity may prepare DOE/NRC F 741 in paper form if coordinated with the DOE CSA.
- Such facilities are encouraged to convert to electronic form preparation in coordination with the NMMSS operator.

Either Method

- Regardless of method used, nuclear material types, elements, and isotopes to be reported, their respective reporting units will be as specified in table XV-1.
- For each detail line of shipper/receiver data entries on DOE/NRC F 741, material quantities reported by assay may be summarized, but only within detailed MT assay ranges (e.g., for enriched uranium, within 10 to 20 percent U-235 or within 80 to 92 percent U-235, as appropriate) required for reporting inventory (see chapter XIII, Inventory Reporting).

Data sent to NMMSS will agree on a line-for-line-basis with data sent between the shipper and receiver on DOE/NRC F 741, or electronic equivalent.

58. Safeguards and security personnel with the responsibility for MC&A must demonstrate a working level knowledge of the requirements for nuclear material balance reporting.

a. Describe the instructions to DOE license-exempt contractors, the NRC, and Agreement State licenses that are DOE contractors for the preparation and distribution of DOE/NRC F 742, Material Balance Report (MBR), or its electronic equivalent.

The following is taken from DOE M 470.4-6 chg 1.

Do not send a copy of DOE/NRC F 742 data to the NMMSS if arrangements have been made to receive a NMMSS-generated MBR or if reporting electronically. If DOE/NRC F 742 is prepared in paper form, copies of each will be distributed to NMMSS and also to other recipients, if any, according to instructions provided by the DOE CSA.

b. Describe the special procedures for facilities that have been selected under the terms of either the U.S./International Atomic Energy Agency (IAEA) Safeguards Agreement or Protocol for the preparation and distribution of DOE/NRC F 742, MBR, or its electronic equivalent.

The following is taken from DOE M 470.4-6 chg 1.

Special procedures must be used to implement some of the reporting requirements of the U.S./IAEA Safeguards Agreement. DOE M 470.4-6 chg 1, chapter XII, provides instructions for use of these special procedures for facilities that have been selected under the terms of either the U.S./IAEA Safeguards Agreement or Protocol. Such facilities should note that all requirements and procedures in the main body of DOE M 470.4-6 chg 1 apply in addition to the special requirements of chapter XII.

DOE/NRC 742 or its electronic equivalent will be completed by filling in the numbered blocks or lines listed in DOE M 470.4-6 chg 1, chapter XI plus the fields that follow.

- Block 7, DOE/NRC F 470M. Place an X in the appropriate box. Concise notes are optional unless required by facility attachments or transitional facility attachments. DOE/NRC F 740M, Concise Note, will be used by selected facilities to supplement material balance data on DOE/NRC F 742.
- Line 22, From Other Materials. For each entry on this line, fill in the appropriate two-character inventory change type (ICT) code (see DOE M 470.4-6 chg 1, table XV-18) in the space provided to indicate the source and destination material balances for the inventory change being reported. The IAEA does not require the reporting of category changes for enriched uranium.
- Line 30, Receipts Reported to DOE/NRC on DOE/NRC F 741. Reporting of receipts of material for facilities selected by the IAEA may require additional procedures. Contact the Office of Resource Management for further information.

- Line 51, Shipments Report to DOE/NRC on DOE/NRC F 741. Shipments of material for facilities selected by the IAEA may require additional procedures. Contact the Office of Resource Management for further information.
- Line 71, Degradation to Other Materials. For each entry on this line, enter the appropriate two-character ICT code (degradation), as shown in DOE M 470.4-6 chg 1, table XV-18, in the space provided to indicate the source and destination material balances for the inventory change being reported.

59. Safeguards and security personnel with the responsibility for MC&A must demonstrate a working level knowledge of the requirements for inventory reporting.

a. Discuss the instructions to license-exempt contractors, the NRC, and Agreement State licensees that are contractors for the preparation and distribution of DOE/NRC F 742C, Physical Inventory Listing.

The following is taken from DOE M 470.4-6 chg 1.

The instructions that follow correspond to those data fields and columns appearing on DOE/NRC F 742C. To obtain instructions for electronic reporting, contact the NMMSS operator. Whether reporting electronically or by DOE/NRC F 742C, the following instructions apply:

- Block 1, Name and Address. Enter reporting facility information.
- Block 2, DOE/NRC Form 740M. Check the appropriate box.
- Block 3, RIS. Enter the RIS of the reporting facility.
- Block 4, Inventory Date. Enter the ending date on which the MBR is based.
- Block 5, Process Code. Leave blank.
- Block 6, Correction ID. Leave blank.
- Block 7, License Number. Leave blank.
- Block 8, Batch Data.
- Block 8l, Material Type. Enter the material type code that reflects the material assay range unless the material is being reported under one of the following categories:
  - Losses—weapons and non-weapons—42 U.S.C. 2121(b), *Material for DoD Use*. For material reported by assay range, use the appropriate material type code from DOE M 470.4-6 chg 1, table XV-17.
  - Losses—42 U.S.C. 2121(c), *Sale, Lease or Loan to Other Nations of Materials for Military Applications*. For material reported by assay range, use the appropriate material code from DOE M 470.4-6 chg 1, table XV-17.
  - Scrap data (lines 971-974). If reporting scrap generated onsite, recovered onsite, recategorized onsite, or declared to the Central Scrap Management Office, use the appropriate material type code from DOE M 470.4-6 chg 1, table XV-17.
- Block 8b, Composition Code. Enter the code that identifies the physical and/or chemical form of the nuclear material at the time the transaction occurs. A complete set of composition codes, which consists of available nuclear material composition

codes and descriptions, may be obtained from the NMMSS operator (referred to as Composition of Ending Inventory (COEI) codes).

- Block 8c, Element Weight. Enter element weights as per the instructions in DOE M 470.4-6 chg 1, chapter XI for DOE/NRC F 742.
- Block 8d, Isotope Weight. Enter isotope weights as per the instructions in DOE M 470.4-6 chg 1, chapter XI for DOE/NRC F 742.
- Block 8e, DOE Project Number. Make no entry unless reporting DOE-owned material.
- Block 8f, Scrap Program. Leave blank.
- Block 8g, Weight Percent Isotope. Leave blank.
- Block 8h, Owner Code. Enter the appropriate code from DOE M 470.4-6 chg 1, table XV-3.
- Block 8i, Sequence Number. Enter the line sequence numbers consecutively. Do not repeat or skip numbers.
- Block 8j, Batch Name. No entry required. Can be used locally by reporting facility.
- Block 8k, Number of Items. Leave blank.
- Block 8l, Key Measurement Point. Leave blank.
- Block 8m, Measurement ID (measurement basis, other measurement point, measurement method). Leave blank.
- Block 8n, Entry Status. Leave blank.
- Block 8o, MBA. Leave blank.
- Block 8p, Site/Item Description Code. Leave blank.
- Block 9, Totals. Enter the total inventory reported in the above categories. This total must agree with the sum of the quantities entered on line 80 and 81 on the DOE/NRC F 742.
- Block 10, Signature. The report, if submitted as a hard copy, will be signed by an authorized representative of the facility.
- Block 11, Title. Enter the title of the person submitting the report.
- Block 12, Date. Enter the date the report was submitted.

Provide the physical inventory listing to NMMSS and to others as specified by the DOE CSA.

b. Describe the use of the following:

- **Nuclear material composition codes and descriptions**
- **Authorized profiles of inventory data**
- **Nuclear material type codes**

The following is taken from DOE M 470.4-6 chg 1.

Nuclear Material Composition Codes and Descriptions

Nuclear material composition codes and descriptions may be found in the inventory profile report (I-17 report from NMMSS) developed by DOE, their contractors, and NRC. The report is to be used as a guide for reporting the inventory composition code on DOE/NRC F

742C. A facility selected by the IAEA will report the IAEA material description code as appropriate.

Authorized Profile of Inventory Data

The inventory profile report (I-17) will be updated by the NMMSS operator. The report is divided into an inventory data section (lines 005–899) and a miscellaneous data section (lines 900–998). Each section is arranged according to process, usage, chemical, and physical form. The report is designed so that additional lines can be added as necessary to both the inventory data section and the miscellaneous data section. Any proposed changes in the format are to be reported to the Office of Resource Management.

Nuclear Material Type Codes

Nuclear material type codes, descriptions, and reporting units are given in DOE M 470.4-6 chg 1, table XV-2. See table 3 below.

Table 3. Nuclear material types codes

Type Code	Type Description	Reporting Unit	Type Code	Type Description	Reporting Unit
	Uranium Depleted in U-235		44	Americium 241	gm
10	Total		45	Americium 243	gm
11	<0.21% U-235	kg	46	Curium	gm
12	0.21 to <0.24% U-235	kg	48	Californium	microgram
13	0.24 to <0.26% U-235	kg		Plutonium	
14	0.26 to <0.28% U-235	kg	50	Total	gm
15	0.28 to <0.31% U-235	kg	51	<4.00% Pu-240	gm
16	0.31 to <0.50% U-235	kg	52	4.00<7.00% Pu-240	gm
17	0.50 to <0.60% U-235	kg	53	7.00<10.00% Pu-240	gm
18	0.60 to <0.710% U-235	kg	54	10.00<13.00% Pu-240	gm
	Uranium Enriched in U-235		55	13.00<16.00% Pu-240	gm
20	Total		56	16.00<19.00% Pu-240	gm
21	>0.712 to <0.90% U-235	gm	57	19.00% and above Pu-240	gm
22	0.90 to <1.15% U-235	gm		Lithium Enriched in Li-6	
23	1.15 to <1.60% U-235	gm	60	Total	kg
24	1.60 to <2.00% U-235	gm	61	>Normal (7.42%) to <55.00%	kg
25	2.00 to <2.60% U-235	gm	62	55.00 to <80.00%	kg

Type Code	Type Description	Reporting Unit	Type Code	Type Description	Reporting Unit
26	2.60 to <2.90% U-235	gm	63	80.00% and above	kg
27	3.10 to <3.40% U-235	gm		Uranium Enriched in U-233	
28	3.10 to <3.40% U-235	gm	70	Total	gm
29	3.40 to <3.90% U-235	gm	71	<5 ppm U-232	gm
30	3.90 to <4.10% U-235	gm	72	5 to <10 ppm U-232	gm
31	4.10 to 5.00% U-235	gm	73	10 to <50ppm U-232	gm
32	5.00 to <10.00% U-235	gm	74	50 ppm and above U-232	gm
33	10.00 to <20.00% U-235	gm	81	Normal U	
34	35.00 to <45.00% U-235	gm		Total	
35	35.00 to <45.00% U-235	gm		0.710 to ≤0.712% U-235	kg
36	45.00 to <80.00% U-235	gm	82	Np 237 Total	gm
37	80.00 to <92.00% U-235	gm	83	Pu Total	gm to tenth
38	92.00 to <94.00% U-235	gm	86	D_2 Total	kg to tenth
39	94.00% and above U-235	gm	87	Tritium Total	gm to hundredth
	Plutonium 242		88	Thorium Total	kg
40	Total	gm	89	U in Cascades Total	gm
41	20% thru 60%	gm	90	This series is available for local use	

Source: DOE M 470.4-6 chg 1.

c. Describe the procedures for the following:
- **Reconciliation of facility data with NMMSS**
- **Preparation of DOE/NRC F 742C**
- **Distribution of DOE/NRC F 742C data**

The following is taken from DOE M 470.4-6 chg 1.

Reconciliation of Facility Data With NMMSS

Reconciliation of facility data is required annually of facilities after submission of September 30 inventory data. The process is as follows:

- The facility submits its inventory for the period just ended and is provided with the results of processing in NMMSS.

- Preliminary reports are available upon request from the NMMSS for facility use in comparing facility data to NMMSS balances.
- The data at the facility and comparable data in the NMMSS are compared and adjustments are made to the facility books or to NMMSS, as appropriate, regarding balances of material by type, ownership code, and project number (if DOE-owned), and foreign obligation, if applicable.
- Reconciliation of facility data with NMMSS more frequently than the annual periods required above is permissible.

Preparation of DOE/NRC F 742C

The following is taken from DOE M 470.4-6 chg 1.

Instructions for preparation of DOE/NRC F 742C:

- Block 1, Name and Address. Leave blank.
- Block 2, Attachment to. Place a check mark or an X in the appropriate box to indicate whether this explanatory information will be attached to a DOE/NRC F 741, 742, or 742C.
- Block 3, RIS. Enter the RIS for your facility to which the explanatory information in this report applies.
- Block 4, Reporting Period. Complete this block if 2b or 2c was checked, indicating that this concise note is attached to a DOE/NRC F 742C, Physical Inventory Listing. Enter the beginning and ending dates of the reporting period as shown on DOE/NRC F 742 or F 742C.
- Block 5, Transaction Data. Complete this block only if box 2a was checked, indicating that this F 740M is attached to a DOE/NRC F 741. All entries in this block must be identified to those on the DOE/NRC F 741. Fill in the blocks as follows:
  - Block 5a. Enter shipper's RIS.
  - Block 5b. Enter receiver's RIS.
  - Block 5c. Enter the unique transaction number.
  - Block 5d, Correction Number. Used when DOE/NRC F 741 is a correction to a previous report.
  - Block 5e, Processing Code. Enter the same code as was used in the DOE/NRC F 741.
  - Block 5f, Action Code. If a DOE/NRC F 740M is attached enter the same action code as in block 6 of the DOE/NRC F 741. Otherwise enter action code M.
- Block 6, Reporting Date. Complete this block if box 2a or 2c was checked. Copy the date shown on DOE/NRC F 741 or 742C.
- Block 7. The actual explanatory data and the other data necessary to link the explanatory data to the parts of the report to which they apply. Complete this block as follows:
  - Block 7a, Line Number. Enter the consecutive number beginning with one (01) for each explanatory reference.
  - Block 7b, Entry Reference.

- If the explanatory information entered on this line of the DOE/NRC F 740M applies to the entire DOE/NRC F 741, 742, or 742C, enter the words, "Whole Report."
- If the explanation applies to the data on a specific batch on a DOE/NRC F 741 or 742C, copy the batch name exactly as it appears on DOE/NRC F 741 or 742C.
- If the explanation applies to a specific material balance category on a DOE/NRC F 742, enter the two-digit number of the material balance category.
- If the explanation applies to material balance categories 11, 30, 42, 43, or 51, enter the RIS shown on the line of the DOE/NRC F 742.
- If the explanation applies to categories 22 or 71, enter the 2-character ICT as shown on that line of the DOE/NRC F 742.
- If DOE/NRC F 740M action code is M, enter "General."

  - Block 7c, Text of Concise Note. Enter any 43 characters, letters, numbers, or special characters per line. Up to 99 lines of text may be used for any one explanation.

- Block 8. The DOE/NRC F 740M is to be signed by an authorized representative of the facility.
- Block 9. Enter the title of the person signing the form.
- Block 10. Enter the date the form was signed.
- Computer-Readable Format. DOE/NRC F 740M may be put into computer-readable format following additional guidance in NMMSS Reports D-22 and D-23.

Distribution of DOE/NRC F 742C Data

Distribution of DOE/NRC F 742C data:

- The Concise Note will be submitted at the same time as the submission of the data to which the Concise Note refers.
- If associated with a DOE/NRC F 741, 742, and/or 742C, copies of DOE/NRC F 740M will be attached as applicable.
- Under certain circumstances, a DOE/NRC F 740M can be submitted as a standalone document (e.g., to comply with IAEA reporting requirements).

G CYBER SECURITY (CS)

Competencies and supporting knowledge and skills for Section G, Cyber Security, are derived from the following DOE Orders, manuals, and guides.

- DOE M 205.1-4, National Security System Manual
- DOE M 205.1-5, Cyber Security Process Requirements Manual
- DOE M 205.1-6, Media Sanitization Manual
- DOE M 205.1-7, Security Controls for Unclassified Information Systems Manual
- DOE M 205.1-8, Cyber Security Incident Management Manual
- DOE O 205.1A, Department of Energy Cyber Security Management
- DOE P 205.1, Departmental Cyber Security Management Policy

60. Safeguards and security personnel with the responsibility for CS must demonstrate a working level knowledge of the CS Program.

a. Discuss the DOE Cyber Security Plan and the genesis of it.

The following is taken from DOE O 205.1A.

Senior DOE management is responsible for ensuring implementation of the DOE cyber security program and the respective Program cyber security plans (PCSPs) under their purview. Requirements and responsibilities promulgated in the PCSP will flow down from senior DOE management to all subordinate organizational levels.

Departmental elements must use a documented risk-based approach, according to their applicable PCSP, to make informed decisions for protecting information and information systems under their purview, including the adequacy and maintenance of protection, cost implications of enhanced protection, and acceptance of risk.

PCSPs are living documents that must be developed, approved, and maintained to comply with Federal Information System Management Act (FISMA), Presidential directives and EOs, OMB directives, Federal Information Processing Standard (FIPS), policies promulgated by the Committee on National Security Systems (CNSS), departmental policies, and DOE CIO CS technical and management requirements (TMRs). PCSPs must be reviewed, updated, and reapproved at least every 2 years.

Senior DOE management or their designees must maintain approved copies of PCSPs for auditing and monitoring purposes. Within 90 days of issuance, senior DOE management must implement DOE O 205.1A and develop PCSPs.

b. Discuss the roles and responsibilities of Federal and contractor personnel as they relate to the CS Program and the onsite management of the program.

Federal Personnel

The following is taken from DOE O 205.1A.

Senior DOE Management has direct responsibility and accountability for

- issuing direction for implementing CS within their respective organizations;
- determining, assessing, and documenting program-unique threats and risks (in addition to those presented in the departmental CS threat statement and risk assessment); and
- developing PCSPs for the implementation of CS requirements in all organizations under their purview.

At a minimum, Power Marketing Administration protections must also be in accordance with North American Electric Reliability Council standards.

Contractor Personnel

The following is taken from DOE M 205.1-5 admin chg 2, *Cyber Security Process Requirements Manual*, attachment 1.

Regardless of the performer of the work, the contractor is responsible for implementing and complying with the requirements of this CRD and the applicable senior DOE management PCSP.

The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements.

Contractor managers or system owners may specify and implement additional requirements to address specific risks, vulnerabilities, or threats within its operating unit/systems.

c. Discuss the site's cyber risk management process—including the threat and risk statements and how they are integrated into the site's processes.

The following is taken from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30.

Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment. The system authorizing official is responsible for determining whether the remaining risk is at an acceptable level or whether additional security controls should be implemented to further reduce or eliminate the residual risk before authorizing the IT system for operation.

The head of an organizational unit must ensure that the organization has the capabilities needed to accomplish its mission. These mission owners must determine the security capabilities that their IT systems must have to provide the desired level of mission support in the face of real-world threats. A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential security capabilities.

Minimizing negative impact on an organization and the need for sound basis in decision-making are the fundamental reasons organizations implement a risk management process for their IT systems. An IT system's system development life cycle (SDLC) has five phases: initiation, development or acquisition, implementation, operation or maintenance, and disposal. In some cases, an IT system may occupy several of these phases at the same time. However, the risk management methodology is the same regardless of the SDLC phase for which the assessment is being conducted. Risk management is an iterative process that can be performed during each major phase of the SDLC. NIST SP 800-30, table 2-1 describes the characteristics of each SDLC phase and indicates how risk management can be performed in support of each phase.

d. Discuss the site's cyber configuration management program.

The following is taken from DOE Cyber Security Technical and Management Requirements, Configuration Management (TMR-8).

DOE Order 205.1A, *Department of Energy Cyber Security Management*, charges senior DOE management to implement CS within their respective organizations, based on their determination, assessment, and documentation of DOE and program-unique threats and risks. In carrying out this charge, senior DOE management is required by the Order to develop a PCSP that defines CS requirements for all subordinate organizations and programs.

Configuration management (CM) applies administration, technical direction, and surveillance to identify and document functional and physical characteristics of a configuration item, control changes, record and report change processing and implementation, and verify compliance with specified requirements.

Senior DOE management is responsible for developing, documenting in the PCSP, and implementing CM policies and processes for all operating units, programs, and systems. The senior DOE management PCSP is to describe the CM process to include the following:

- Configuration Management documentation, including SSPs, contingency plans, user and administrator guidance, system component inventory, CM plan, and security testing and evaluation procedures
- Identification of the roles and responsibilities for change approval/disapproval to establish a new baseline
- Policy and processes for security CM for each information system for configuration documentation, change control and tracking, and approval of configuration changes to

all national security systems and other information systems in security categories moderate and high to include at least the following:

- Information system and configuration item unique identification and labeling
- Design documentation, including system specification and configuration item specification(s)
- Configuration change identification, tracking, control, and history
- Configuration status accounting to track changes from identification to implementation to produce a new baseline
- Security configuration checklist for operating system software, application software, and hardware platforms
- Configuration auditing to trace modifications to configuration items for authorized changes
- Integration of vulnerability and patch management processes
- Documentation of configuration change control methodology and tools used
- Documentation of the methodology and tools used to monitor configuration changes

e. Discuss the following as they pertain to CS:

- **Deviation process**
- **Incident management process**
- **Information condition process**
- **Vulnerability management**
- **Foreign national access**
- **Password generation, protection, and use**
- **Portable electronic devices**
- **Wireless technologies, remote access, and peer-to-peer networking technologies**
- **Training and awareness**
- **Federal and contractor self-assessment processes**
- **Contingency planning and disaster recovery**
- **Clearing, purging, and destroying media and associated Federal approval roles**

Deviation Process

The following is taken from DOE M 205.1-5 Admin chg 2.

Exemptions are approved deviations from a requirement in DOE M 205.1-5 Admin chg 2 that may create security vulnerability. Exemptions will be approved only when correction of the condition is not feasible or cost effective and compensatory measures are inadequate to preclude the acceptance of risk.

Incident Management Process

The following is taken from DOE M 205.1-8 Admin chg 2.

DOE M 205.1-8 Admin chg 2, *Cyber Security Incident Management Manual*, establishes the minimum requirements for a structured CS incident management process for identifying,

categorizing, containing, reporting, and mitigating CS incidents involving DOE information and information systems operated by DOE or by contractors on behalf of the Department.

Information Condition Process

The following is taken from DOE CIO Guidance CS-20.

The DOE information condition (INFOCON) process is a structured, coordinated approach to react to adversarial attacks on DOE information, computer systems, and telecommunication networks and systems. The intent of the INFOCON is to determine, assess, and communicate information regarding the risk of cyber attacks and define organizational defensive responses to reduce vulnerability, increase response capability, and mitigate sustained damage to DOE information and infrastructure.

Vulnerability Management

The following is taken from NIST SP 800-40.

Patch and vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization. The expected result is to reduce the time and money spent dealing with vulnerabilities and exploitation of those vulnerabilities. Proactively managing vulnerabilities of systems will reduce or eliminate the potential for exploitation and involve considerably less time and effort than responding after exploitation has occurred.

Foreign National Access

The following is taken from DOE O 142.3 chg 1.

Foreign national access to DOE sites, programs, information, and technologies will be approved provided the access is needed to support the program objectives of DOE and/or U.S. national interests.

Password Generation, Protection, and Use

The following is taken from FIPS Publication 181.

A password is a protected character string used to authenticate the identity of a computer system user or to authorize access to system resources. When users are allowed to select their own passwords they often select passwords that are easily compromised. An automated password generator creates random passwords that have no association with a particular user.

This automated password generator standard specifies an algorithm to generate passwords for the protection of computer resources. This standard is for use in conjunction with FIPS PUB 112, *Password Usage Standard*, which provides basic security criteria for the design, implementation, and use of passwords. The algorithm uses random numbers to select the characters that form the random pronounceable passwords.

Portable Electronic Devices

The following is taken from DOE CIO Guidance CS-14.

Senior DOE management PCSPs are to require operating units to define and document the following:

- Policies prohibiting the use of personally owned portable/mobile devices and media in areas where classified data are discussed or processed
- Policies prohibiting the use of personally owned portable computing devices and media from storing, processing, receiving, or transmitting classified information
- Compliance with Telecommunication: Emission Security (TEMPEST) (study or compromising emanations) and protected transmission system policies for all portable/mobile devices processing, displaying, storing, or transmitting classified information
- Protected transmission systems for all communications to/from the portable/mobile devices accredited for processing classified information
- Policies prohibiting portable/mobile devices accredited for classified processing from downloading or loading any freeware or shareware enhancements or any extraneous software and synchronizing with any unclassified system

Wireless Technologies, Remote Access, and Peer-to-Peer Networking Technologies

The following is taken from NIST SP 800-48.

Wireless local area networks (WLAN) are groups of wireless networking nodes within a limited geographic area, such as an office building or building campus, that are capable of radio communication. WLAN are usually implemented as extensions to existing wired local area networks (LAN) to provide enhanced user mobility and network access.

Legacy WLAN technologies present unique security challenges beyond those encountered with their wired network counterparts. In addition to facing the same threats that wired networks face, legacy WLAN are also threatened by attackers that can intercept WLAN transmissions through the air. To attempt to breach a WLAN, an attacker simply needs to be within range of the wireless transmissions.

The ad hoc mode of operation, also known as peer-to-peer mode, is possible when two or more stations are able to communicate directly to one another. Devices can communicate with each other in a peer-to-peer fashion without any wireless infrastructure or wired connections.

An alternative method of achieving confidentiality and integrity protection is using a virtual private network (VPN). A VPN is a virtual network, built on top of existing physical networks that can provide a secure communications mechanism for data and internet protocol information transmitted between networks. VPNs are often used to facilitate the secure transfer of sensitive data across public networks, such as Internet, for remote access, telework, and other situations involving connecting to multiple locations.

Training and Awareness

The following is taken from National Security Telecommunications and Information Systems Security (NSTISSI) Number 4011.

Education, training, and awareness may be the most prominent security measures for only by understanding the threats and vulnerabilities associated with our proliferating use of automated information systems can we begin to attempt to deal effectively with other control measures.

Federal and Contractor Self-Assessment Processes

The following is taken from DOE P 226.1A.

DOE's oversight policy incorporates a philosophy that relies upon three important elements: a critical and honest self-assessment by Federal and contractor organizations; line management reviews, such as inspections, surveillances, surveys, and walkthroughs that test systems and the validity of the self-assessment; and independent oversight reviews. The keystone of this policy is the self-assessment, which puts accountability and responsibility at the appropriate organizational level (both Federal and contractor).

Contingency Planning and Disaster Recovery

The following is taken from NIST SP 800-34.

NIST SP 800-34, *Contingency Planning Guide for IT Systems*, provides instructions, recommendations, and considerations for government IT contingency planning. Contingency planning refers to interim measures to recover IT services following an emergency or system disruption.

As suggested by its name, the disaster recovery plan (DRP) applies to major, usually catastrophic, events that deny access to the normal facility for an extended period. Frequently, DRP refers to an IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency. The DRP scope may overlap that of an IT contingency plan; however, the DRP is narrower in scope and does not address minor disruptions that do not require relocation. Dependent on the organization's needs, several DRPs may be appended to the business continuity plan.

Clearing, Purging, and Destroying Media and Associated Federal Approval Roles

The following is taken from DOE M 205.1-6 Admin chg 2.

Clearing: The level of media sanitization that would protect the confidentiality of information against a robust keyboard attack. For example, overwriting is an acceptable method for clearing media.

Purging: The level of media sanitization that removes data in such a way that it cannot be reconstructed and renders data unrecoverable by laboratory attack methods.

Destruction: The result of actions taken to ensure that media cannot be reused as originally intended and information is virtually impossible or prohibitively expensive to recover.

f. Discuss the Cyber Security Program Plan (CSPP), including the approvals and review timeframes.

The following is taken from DOE O 205.1 (archived)

Cyber Security Plan Development and Maintenance. PCSPs, CSPPs and their associated security plans must be developed, approved, and maintained in accordance with applicable directives. PCSPs and CSPPs must be reviewed in accordance with FISMA and updated as needed when operational considerations (e.g., risks, threats, general support system configurations, vulnerabilities, or DOE CS directives) change significantly, but not less frequently than every two years. Security plans and CSPPs that function as security plans must be completed annually. Heads of DOE elements will maintain approved copies of PCSPs and CSPPs for audit and monitoring purposes with the ability to provide copies of the plans and referenced supporting material to authorized requestors within two business days from the date of request.

g. Discuss how telecommunications security integrates with CS.

This is discussed in DOE M 205.1-3 (OUO) which is a controlled publication.

61. Safeguards and security personnel with the responsibility for CS must demonstrate a working level knowledge of the Federal planning processes as well as the contractor feedback processes (i.e., oversight) as it pertains to the CS budget and oversight.

a. Discuss the process between the site office, the contractor site, and headquarters in terms of planning, prioritizing, submission, and periodic reviews.

The following is taken from DOE O 205.1A.

OMB Circular A-11, *Planning, Budgeting, Acquisition of Capital Assets, Strategic Plans, Performance Plans*, provides guidance on budget submissions; instructions on budget execution, integrating Agencies' budget and accounting functions, and improving the quality of financial information in accordance with the Government Performance and Results Act of 1993 and other laws; and specific steps that agencies must take to integrate budget and performance, a key part of the President's management agenda.

b. Discuss the current Headquarters Program Execution Guidance and how it is integrated with the site's implementation plans and the Performance Execution Plan (PEP).

The following is taken from DOE G 413.3-15.

The PEP is the governing document that establishes the means to execute, monitor, and control projects which are subject to DOE O 413.3A chg 1, *Program and Project Management for the Acquisition of Capital Assets*.

c. Discuss the methodology used to provide contractors feedback regarding their CS performance.

The following is taken from DOE P 205.1.

Monitor and evaluate the effectiveness of the departmental CS management. Feedback information (performance measures and testing) on the adequacy of CS is gathered, opportunities for improving CS effectiveness are identified and implemented, line and independent oversight is conducted, and, if necessary, enforcement actions occur. Sharing successes and lessons learned is key to implementing successful risk management programs consistently across a variety of DOE/NNSA organizations.

Awareness is promoted throughout the organization. Users are continually educated to understand the risks (threats and vulnerabilities) and provided the skills to practice the related procedures and controls to mitigate the risks that are under their control.

d. Discuss how Federally-issued; including those from Headquarters, the Office of Health, Safety, and Security, the Office of the Inspector General, the Government Accountability Office; etc., findings/deficiencies are tracked and evaluated.

The following is taken from DOE M 470.4-1 chg 1.

Findings are any validated program deficiency (failure to meet a performance or compliance requirement) regardless of source. Findings may be reflected in documents resulting from internal and external reviews, audits, appraisals, and other sources (e.g., OA, Government Accountability Office [GAO], IG, previous surveys, self-assessments, etc.).

All open findings must be reviewed during the survey or self-assessment to validate the status of corrective action and to evaluate the impact on the existing S&S program.

Findings identified during the current survey or self-assessment must be reported immediately to the departmental element and contractor line management if a vulnerability to national security, classified information or matter, nuclear materials, or Department property results, or may result, in a programmatic impact to the Department. Findings identified during a survey or self-assessment, even if closed during the survey or self-assessment activity, must be documented in the associated report.

Findings and deficiencies, regardless of source, and corrective action plans (milestones and estimated completion dates) must be entered into SSIMS according to SSIMS guidelines and tracked until closed. Quarterly status reports must be entered into SSIMS by January 15, April 15, July 15, and October 15, of each year. Self-assessment deficiencies are not required

to be entered into SSIMS; however, a local mechanism/system must be used to track these deficiencies and corrective action until closed.

Trending evaluations must be considered in the resolution of findings in the subtopical area of program management to determine if systemic and systematic causal factors exist within the S&S program. Results of this evaluation that indicate negative trends must be analyzed to ensure corrective action plans address root causes and the need to ensure continuous improvement of the S&S program.

62. Safeguards and security personnel with the responsibility for CS must demonstrate a working level knowledge of the associated processes.

a. Discuss the Plan of Actions and Milestones (POAM) process, including the types of issues tracked and how those issues are determined.

The following is taken from DOE M 205.1-5 admin chg 2.

All CS weaknesses identified for national security or unclassified information systems requiring corrective action will be incorporated into the POA&M process, whether or not a corrective action plan has been prepared. At a minimum, each POA&M will contain the fields required by the OMB/DOE for quarterly reporting.

POA&M management:

- POA&M activities for each operating unit/program/system must be reviewed and assessed on at least a quarterly basis.
- POA&Ms will be updated as needed when there are changes in roles and responsibilities; executive, legislative, technical or departmental guidance; when vulnerabilities, risks or threats occur; and if new findings are identified in an audit, review, or self-assessment.
- Corrective action plans must be prepared for all POA&Ms that require more than one year to complete.

POA&M Reporting:

- In accordance with the FISMA reporting requirements, senior DOE management will report quarterly POA&M status for all operating units, programs, and classified and unclassified information systems through the Office of the CIO.
- At a minimum, POA&M reporting will include:
  - program and system-level findings for all classified and unclassified systems, including those identified by the Office of Health, Safety, and Security; GAO; and IG;
  - any weaknesses and open action items resulting from internal program and system reviews;
  - type 1 incidents; and

- self-assessments, risk assessments, security plans, privacy impact assessments, certification and accreditation (C&A), contingency plans, and implementation of PCSP and other CS-related requirements (e.g., requirements in program-specific directives or contract documents).

b. Define a Federal Information Security Management Act (FISMA) of 2002 system.

The following is taken from Title III-Information Security, section 301, 3542, *Definitions*.

The term national security system means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

- The function, operation, or use of which
  - involves intelligence activities
  - involves cryptologic activities related to national security
  - involves command and control of military forces
  - involves equipment that is an integral part of a weapon or weapons system

    - is critical to the direct fulfillment of military or intelligence missions or
    - is protected at all times by procedures established for information that have been specifically authorized under criteria established by an EO or an Act of Congress to be kept classified in the interest of national defense or foreign policy
- This does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

c. Discuss how the site tracks and manages FISMA systems.

The following is taken from DOE CIO Guidance CS-6.

In accordance with FISMA reporting requirements, all CS weaknesses requiring corrective action are to be incorporated into the POA&M process, whether or not a corrective action plan has been prepared. The lack of self-assessments, risk assessments, security plans, C&A, contingency plans, and implementation of other requirements (including the PCSP) must be included. Senior DOE management PCSPs are to require operating units to

- develop, implement, and manage POA&Ms for their CS program (including projects planned as a result of program improvements) and systems they own and operate that have identified security weakness.
- track, maintain, review, and prioritize POA&M activities on at least a quarterly basis. The procedure should include a regular review of the POA&Ms and verification that all applicable findings are being tracked. In addition to regularly scheduled reviews, a POA&M assessment is to be completed when there are changes in roles and responsibilities, or new executive, legislative, technical or departmental guidance is issued; changes in vulnerabilities, risks or threats occur; interim authority to operate

(IATO) exceeds one hundred eighty days; and/or new vulnerability findings are identified in an audit, review, or self-assessment.

d. Discuss the system inventory process.

The following is taken from DOE M 205.1-7 Admin chg 2.

The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information. The organization determines the appropriate level of granularity for the information system components included in the inventory that are subject to management control (i.e., tracking, and reporting). The inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner). The component inventory is consistent with the accreditation boundary of the information system.

The organization updates the inventory of information system components as an integral part of component installations. The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

63. Safeguards and security personnel with the responsibility for CS must demonstrate the ability to conduct oversight in accordance with the site's policies, including programmatic reviews, performance tests, and reviews of technical processes.

a. Demonstrate the ability by conducting a CS programmatic review documented in accordance with site procedures.

b. Demonstrate the ability by conducting a CS performance test documented in accordance with site procedures.

c. Demonstrate the ability by conducting a CS review of a selected technical implementation documented in accordance with site procedures.

These are performance-based KSAs. The Qualifying Official will evaluate their completion.

64. Safeguards and security personnel with the responsibility for CS must demonstrate a working level knowledge of the *Certification and Accreditation (C&A) Processes for Information Systems* or its subsequent revisions.

a. Describe the national drivers for the C&A process.

The following is taken from the DOE CIO Guide 205.1-2.

Federal agencies are required to establish a C&A process to ensure that adequate security controls are provided for all Department information systems. The proper implementation of the C&A process will ensure that all applicable requirements have been integrated into the development and operational processes. The Department expects that all systems complete C&A prior to going operational, (i.e., processing live data or information). DOE CIO Guide 205.1-2, *Certification and Accreditation Guide*, describes the minimum expectations for the C&A of information systems within DOE.

DOE CIO Guide 205.1-2 is based upon DOE Cyber Security Policy, FIPS 199, *Standards for the Security Categorization of Federal Information and Information Systems*, FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, and NIST SP 800-37 Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, and other applicable departmental and Federal IT security laws and regulations.

b. Describe the C&A process, including approvals and associated timeframes.

The following is taken from DOE M 205.1-5 Admin chg 2.

The C&A of all DOE information systems must be performed every three years or after any significant system changes that require that the system be re-accredited.

The C&A process will include the following phases and specify the required formats for documentation in each phase.

- C&A initiation phase allows an organization to determine the information system security status quickly and identify changes that have to be made to attain or maintain compliance with the Federal, departmental, and senior DOE management PCSP requirements.
  - Preparation task steps will include the following:
    - Describe the information system in the SSP.
    - Categorization of the information system using the process described by NIST FIPS 199 or DOE M 205.1-4, as applicable.
    - Identify and document potential threats, vulnerabilities, and risks.
    - Document implemented and planned security controls in the SSP.
  - Notification and resource identification task steps will include the following:
    - Determine the resources needed to accomplish S&A.
    - Create a POA&M for execution and budget input and provide it to the DAA.
    - Notify all stakeholders that C&A activities are to be accomplished.
  - SSP analysis and acceptance task steps will include the following:
    - Complete an independent review of the SSP, conducted or overseen by the certification agent and DAA. The review will include a verification that: the

system security categorization is correct; the documented vulnerabilities, threats, and associated risks are accurate; and the implemented and planned controls are sufficient.
- Update the SSP with any findings from the independent reviews.
- DAA written approval of the SSP prior to progressing to the next C&A phase.

- The certification phase demonstrates, through the independent validation using specified verification techniques and procedures, the security controls for the information system have been implemented correctly and are effective in their application.
  - Security control assessment task steps will include the following:

    - Define ST&E procedures.
      For a low impact unclassified system, a self-assessment can be substituted for ST&E.
      The ST&E procedures must be approved by the DAA prior to the conduct of control assessment.
      The controls and procedures to be used for future instantiations for site and type forms of accreditation must be included as part of the ST&E procedures.
      If a control fails the ST&E process, the control implementation can be corrected and re-assessed.
    - Assess security controls.
    - Prepare an ST&E report to include test results and recommended POA&M, if applicable.
    - The certification agent will develop the security assessment report.

  - Certification documentation task steps will include the following:

    - Certification agent recommendations to the system owner for correcting any deficiencies or reducing and/or eliminating vulnerabilities identified in the security assessment.
    - Update the SSP and risk assessment.
    - Update the POA&M and create any additional POA&M as needed.
    - Assemble the C&A package for the DAA.
- The accreditation phase determines if remaining vulnerabilities pose an acceptable level of risk.
  - DAA determination of the residual risk.
  - DAA determination if the residual risk is at an acceptable level, and preparation of a final accreditation decision letter. Decision options are:

    - Accreditation. The information system is authorized to operate as specified in the certification package.

- IATO—the information system is authorized to operate but has deficiencies that must be corrected.
  The deficiencies will not present any adverse impacts on the confidentiality of the information on the system.
  The DAA, certification agent, and system owner must agree on the proposed correction and timeframes.
  A POA&M will be prepared for each proposed correction.
  The IATO period must not exceed six months.
  Denial. The information system is not authorized to operate.

- The continuous monitoring phase provides oversight and monitoring of security controls by the system owner on an ongoing basis.
  - Configuration management and control determines security impact of proposed changes to the system.
  - Security control monitoring performs periodic self-assessment of selected technical, operational, assurance, and management security.
  - Status report and documentation tasks steps shall include the following:

    - Update and document in the C&A package changes proposed during this phase.
    - Update the POA&M and create additional POA&Ms, as needed.
    - Report the status of the information system to the DAA.

c. Describe the differences between the "Approval to Operate," "Interim Approval to Operate," and "Interim Approval to Test."

The following is taken from *Information System Certification and Accreditation Process, Approval to Operate.*

Approval to operate is the formal authorization for a system or major application to process information at a specified level of sensitivity in an operational environment. It is based upon validation that a system or major application (MAP) is installed and operated in compliance with Federal law and regulatory guidance, and specified U.S. Agency for International Development security requirements.

The following is taken from CNSS Instruction No. 4009.

Interim Approval to Operate (IATO)—temporary authorization granted by a DAA for an IS to process information based on preliminary results of a security evaluation of the system.

Interim Approval to Test (IATT)—Temporary authorization to test an IS in a specified operational information environment within the timeframe and under the conditions or constraints enumerated in the written authorization.

d. Describe the differences between a Type, Site, and System Accreditation.

The following is taken from DOE CIO Guide 205.1-2.

Type accreditations are used to accredit multiple instances of a MAP or general support systems (GSS) for operation at approved locations with the same type of computing environment but the computing environments may be under different management control.

A site accreditation is an accreditation for a particular site or an enclave. A site accreditation is practical with disparate information systems controlled by a single management authority within a well-defined physical site (e.g., region, business center, building, or floor).

A system accreditation, the most common form of accreditation for an MAP or a GSS, is an accreditation for a single information system or group of components, network, or MAP.

e. Describe system categorization, the consequence of loss, and the methodology used to determine the correct management, operational, and technical controls.

System Categorization

The following is taken from DOE CIO Guide 205.1-2.

The SSP, or an attachment to the plan, must include the security category for the information system based on the impact level for each security objective (confidentiality, integrity, and availability) as described in FIPS 199. The applicable senior DOE management PCSP and NIST SP 800-60, *Information Security*, provide further guidance. The senior DOE management PCSP will specify the process for system categorization.

Consequences of Loss

The following is taken from DOE M 205.1-4.

The technical, operational, and assurance controls that comprise the minimum set of security controls for the system must be documented in the SSP, including any additional implementation information for the control. Any additional controls resulting from adjustments identified during the risk management process must also be included in the SSP.

The SSP must address how the system implements the minimum technical, operational and assurance requirements identified in DOE M 205.1-4. If the consequence of loss (CoL) for confidentiality, integrity or availability has been increased by the senior DOE management or the operating unit or there is a threat not identified in the DOE Cyber Threat Statement, the SSP must describe the implementation of any additional controls.

Common security controls defined in the PCSP or operating unit CS program can be technical (e.g., performed by a single system or device in a network), operational (e.g. the same purging procedure applies to all operating unit systems), or assurance (e.g. the same CM process used for multiple systems). Common security controls must be documented in at

least one approved SSP associated with an accredited information system. The C&A of that system will verify that the control has been correctly implemented and is effective. Use of the control(s) in other information systems requires DAA-approved testing to validate correct implementation of the control(s) in the new information system. Other SSPs may reference that SSP for implementation documentation and certification test results.

Technical Controls

The following is taken from DOE M 205.1-4.

Extensive technical protection measures may be inappropriate and unnecessarily expensive for single-user, stand-alone information systems. Information systems that have one user, are multi-user information systems and are to fully comply with the requirements in DOE M 205.1-4 implemented in the senior DOE management PCSP. Senior DOE management PCSPs are to establish the process for determining which of the management, operational, and technical controls contained in DOE M 205.1-4 are to be applied to stand-alone, single-user information systems in the senior DOE management operating units.

Technical controls rely on the IT resource containing the information. Technical controls are intended to be implemented within the information system through means employing software, hardware, or firmware.

The PCSP must require each operating unit to implement the security audit controls listed in DOE M 205.1-4, table 5, pertaining to the indicated protection index for all national security systems under their responsibility. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them. These controls address the recognizing, recording, storing, and analyzing information related to security relevant activities and the information system security controls and a trusted channel between the information system security controls and other trusted IT products.

Operational Controls

The following is taken from DOE M 205.1-4.

The PCSP must require each operating unit to implement the operational controls listed in DOE M 205.1-4, table 15, pertaining to the indicated protection index for all national security systems under their responsibility. Operational controls are intended to be implemented within the environment in which the information system resides through processes, procedures, or other information systems. Operational controls were constructed for those objectives that rely on physical protection and security processes and for those objectives that are solely security operational issues.

Management

The following is taken from DOE M 205.1-4.

Senior DOE management must develop, and issue to each operating unit, mission-oriented implementation policies for the criteria of DOE M 205.1-4. The senior DOE management PCSPs must require their operating units to implement and maintain at least the minimum requirements in DOE M 205.1-4 for national security systems within 120 days of the release of the PCSP. If an operating unit cannot implement the requirements of DOE M 205.1-4, as documented in the PSCP, by the scheduled milestone, the operating unit must establish a POA&M for implementation of the PCSP requirements. Information systems designated as intelligence systems are subject to the requirements of the Director of National Intelligence and are therefore excluded from the requirements of DOE M 205.1-4.

DOE M 205.1-4 is composed of two chapters that provide direction for the characterization of information, risk management, and security controls to be implemented for national security systems and the responsibilities for managing CS. These chapters address mandatory procedures and management processes.

f. Describe the information groups, their respective consequence of loss, and how this is considered in determining appropriate security controls.

The following is taken from DOE M 205.1-4.

National security information is grouped (information group) based on sensitivity (classification level, category, and need-to-know). The following paragraph describes the information groups used by the DOE in increasing order of sensitivity (TS Restricted Data considered the most sensitive). National security Systems must be categorized based on the most sensitive information group they contain and the impact/CoL if the confidentiality, integrity and/or availability of the information is lost. The impact is determined through a CoL concept that ranks the perceived value of each information group in terms of confidentiality, integrity, and availability. A DOE evaluation has determined a minimum DOE CoL value for each information group.

An information group contains all information types that require similar protection or are similar in content or use. The DOE CIO has identified a minimum set of NSI groups, not including SCI information or information in SAPs. These information groups have been used in assessing the risk to information and in defining the minimum protection criteria for information systems containing each information group. The information groups and sub-groups are:

- Confidential/Secret (C/S)—Information that is classified as C National Security Information, Confidential Formerly Restricted Data, Confidential Restricted Data, Secret National Security Information, or Secret Formerly Restricted Data and does not contain any nuclear weapons data.
- Secret Restricted Data (SRD)—Information that is classified Secret Restricted Data and does not contain any nuclear weapons data.
- Confidential Restricted Data (CRD), Sigmas 1 through 13 (CRD1-13)— Information that is classified as C and identified as Restricted Data, Formerly Restricted Data, or is related to nuclear weapons contains information that falls in at least one of the

sigma categories 1 through 13 as described in DOE Order 5610.2 chg 1, *Control of Weapon Data*, and successors.

- Secret Restricted Data, Sigmas 1 through 13, 15 and 20 (SRD1-13, 15, 20)—Information that is classified as S and identified as Restricted Data and is related to nuclear weapons and contains information that falls within at least one of the sigma categories 1 through 13, 15 and 20 as described in DOE Order 5610.2 and successors.
- Secret Restricted Data, Sigma 14 (SRD14)—Information that is classified as S and identified as Restricted Data or is related to nuclear weapons and contains information that falls within the Sigma 14 category, as described in DOE Order 5610.2, *Control of Weapon* Data (restricted), DOE M 452.4-1A, *Protection of Use Control Vulnerabilities and Design*, and DOE O 457.1, *Nuclear Counterterrorism*, respectively and their successors.
- TS—Information that is classified as TS National Security Information or TS Formerly Restricted Data and does not contain any nuclear weapons data.
- TS Restricted Data (TSRD)—Nuclear Weapons information that is classified TS.

See DOE M 205.1-4, tables 1, 2, and 3 for the criteria used to determine the CoL to confidentiality, integrity, and availability for all information groups. Table 4 provides the results of the DOE evaluation of impact of loss for each NSI group and represents the minimum CoL value for confidentiality, integrity, and availability for each information group.

g. Describe the site's major applications.

This is a performance-based KSA. The Qualifying Official will evaluate its completion.

h. Describe security testing and evaluation as they relate to C&A.

The following is taken from DOE M 205.1-4.

The system owner shall test the information system security controls and document the results. The system owner shall provide test documentation that consists of test plans, test procedure descriptions, expected test results, and the actual test results. The test plans shall identify the security controls to be tested and describe the goal of the tests to be performed. The test procedures shall identify the test to be performed and describe the scenarios for testing each security function. The scenarios shall include any ordering dependencies on the results of other tests. The expected test results shall show the anticipated outputs from a successful execution of the tests. The test results from the system owner execution of the tests shall demonstrate that each tested security control behaved as specified. The system owner shall provide a suitable information system for testing and shall provide an equivalent set of resources to those that were used in the system owner's functional testing of the information system security controls.

The following is taken from DOE CIO Guide 205.1-2.

Security Test & Evaluation Report – A comprehensive evaluation (System Test and Evaluation [ST&E]) of all the management, operational and technical security controls for the information system must be conducted to determine

- the effectiveness of those controls in a particular environment of operation; and
- the vulnerabilities in the system after the implementation of such controls.
- NOTE: For low impact systems, a self-assessment can be substituted for an ST&E.

i. Discuss the risk assessment as it relates to C&A.

The following is taken from DOE M 205.1-4.

The DOE cyber threat statement identifies the threats to DOE information and information systems and the DOE cyber risk assessment provides an assessment of the risks posed by the cyber threats. The DOE cyber threat statement provides an assessment of the threats to DOE (including NNSA) information and information systems and the likelihood that a specified perpetrator will initiate threat activities. The DOE cyber risk assessment evaluates the likelihood of threat activities against each information group and identifies the uncompensated risk to the information group and system on which it resides. The risk management process must be accomplished throughout the system life cycle.

j. Discuss the privacy impact assessment as it relates to C&A.

The following is taken from DOE O 206.1A.

Privacy, like security, should be considered at all stages of the system's life cycle. Departmental elements must also consider the information life cycle in evaluating how information handling practices at each stage may affect an individual's privacy. Privacy impact assessments (PIAs) should be conducted as part of the C&A process. At a minimum, PIAs must be conducted when

- designing, developing, or procuring information systems or IT projects that collect, maintain, or disseminate information in identifiable form;
- initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for ten or more persons;
- significantly modifying an information system.

PIAs should be updated whenever there is a change to the information system that affects privacy or creates new risks to privacy.

k. Describe the Interconnection Security Agreement (ISA) as it relates to C&A.

The following is taken from DOE Program Cyber Security Plan.

A system interconnection occurs when a system connects with another system outside of its accreditation boundary for the purpose of sharing data and other information resources. Significant benefits that can be realized through a system interconnection include: reduced operating costs, greater functionality, improved efficiency, and centralized access to data.

Interconnecting IT systems may also strengthen ties among participating organizations by promoting communication and cooperation.

Despite its advantages, interconnecting IT systems can expose the participating organization to risk. It is critical, therefore, that both parties learn as much as possible about the risks associated with the planned or current interconnection and the security controls that they can implement to mitigate those risks. It also is critical that the parties establish an agreement with each other regarding the management, operation, and use of the interconnection, and that they formally document this agreement. The agreement shall be reviewed and approved by appropriate senior staff from each organization. The risks associated with the interconnection must be approved by the DAA. For interconnected systems that are accredited by the same DAA, the risks associated with connecting the two systems will be documented in the SSPs and approved by the DAA.

l. Describe the approvals associated with a C&A package.

The following is taken from *Information System Certification and Accreditation Process, Approval to Operate*.

Approval is the formal authorization for a system or MAP to process information at a specified level of sensitivity in an operational environment. It is based upon validation that a system or MAP is installed and operated in compliance with Federal law and regulatory guidance, and specified U.S. Agency for International Development security requirements.

See 64c for approvals associated with a C&A package.

65. Safeguards and security personnel with the responsibility for CS must demonstrate the ability to evaluate information system security plans, risk assessments, and issue approval to operate.

a. Demonstrate the ability to evaluate an information systems security plan, including a risk assessment.

b. Demonstrate the ability to accredit a CS system, including conducting an assessment that supports an accreditation decision.

These are performance-based KSAs. The Qualifying Official will evaluate their completion.

66. Safeguards and security personnel with responsibility for CS must demonstrate a working level knowledge of the following concepts, as taken from the Common Body of Knowledge, as they relate to CS and oversight.

a. Describe "access controls" as it relates to CS.

The following is taken from the Inform IT, *Common Body of Knowledge (CBK)*.

Access control is the part of a system used to determine what a user can access. It is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system.

There are two main types of access control methods:

- Discretionary access control is a subjective method, based on a decision made by an individual user. When a user creates a resource such as a file, they can define an ACL that regulates who can have access.
- Mandatory access control is a standardized method of categorizing resources and users based on a predetermined set of criteria overseen by an authority figure.

b. Describe "application security" as it relates to CS.

The following is taken from DOE, *Cyber Security Awareness and Training Program Plan and Essential Body of Knowledge (EBK)*.

System and applications security refers to the principles, policies, and procedures pertaining to integrating information security into an IT system or application during the system SDLC prior to the operations and maintenance phase. This approach ensures that the operation of IT systems and software does not present undue risk to the organization and its information assets. Supporting activities include risk assessment; risk mitigation; security control selection; implementation and evaluation; C&A; and software security standards compliance.

c. Describe "cryptography" as it relates to CS.

The following is taken from NIST 800-21.

Today's IT security environment consists of highly interactive and powerful computing devices and interconnected systems of systems across global networks where Federal agencies routinely interact with industry, private citizens, state and local governments, and the governments of other nations. Consequently, both private and public sectors depend upon information systems to perform essential and mission-critical functions. In this environment of increasingly open and interconnected systems and networks, network and data security are essential for the optimum use of this information.

Cryptography should be considered for data that is sensitive, has a high value, or is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage. Cryptographic methods provide important functionality to protect against intentional and accidental compromise and alteration of data. Some cryptographic mechanisms support confidentiality during communications by encrypting the communication prior to transmission and decrypting it at receipt. These methods provide file/data confidentiality after retrieval from the storage medium. Other cryptographic mechanisms, such as message authentication codes and digital signatures, provide data content integrity and source authentication services. That is, the cryptographic mechanisms permit the user to determine that the entity claiming to be the source of data really is the

source and to determine whether information has been modified since it was last authenticated or signed by its source.

The following is taken from DOE M 205.1-4.

The PCSP must require each operating unit to implement the cryptographic support controls listed in DOE M 205.1-4, table 7, pertaining to the indicated protection index for all national security systems under their responsibility. These controls address the operational use and management of cryptographic keys when the information system implements cryptographic functions.

d. Describe "legal, regulations, compliance, and investigations" as they relate to cyber system.

The following is taken from Inform IT, *Common Body of Knowledge (CBK)*.

The law, investigations, and ethics domain addresses computer laws, regulations, the investigative measures and techniques that can be used to determine if a crime has been committed, methods to gather evidence if it has, as well as the ethical issues and code of conduct for the security professional.

Computers have had an undeniable positive impact on this world; however, the benefits of information systems come with a price: computer crime. Using computers, criminals can access private information, destroy data, steal intellectual property, and more. When these situations occur, it is up to the owner of the system to properly report the crime and ensure that no evidence is destroyed or lost. Unfortunately, the law is often considered a complex body of obscure rules that only lawyers can understand. In addition, the stigma of legal authorities and their overall unpopularity may make users uncomfortable with the prospect of reporting a criminal incident. Others are concerned with the unwanted publicity that might be associated with a public computer crime case. Regardless of what fears or issues a user has, every information-systems professional should be familiar with certain techniques and practices to ensure that evidence is not damaged or lost in the case of an intrusion.

e. Describe "OPSEC" as it relates to CS.

The following is taken from Inform IT, *Common Body of Knowledge (CBK)*.

OPSEC is the practice of putting yourself in your opponent's shoes, and then building a defensive system based on what you discover. The first step is to determine what resources you want to protect. This includes all hardware devices (routers, switches, printers, etc.), software applications, and, most importantly, the users. The second step is to identify the privileges that need to be restricted, and the third step is to identify the available controls that can prevent misuse and abuse of the allotted privileges.

The OPSEC process takes into consideration the following five key principles:

- Identifying critical information

- Analyzing threats
- Assessing vulnerabilities
- Assessing risks
- Applying countermeasures

To apply these principles, OPSEC uses indicators collected via log files, auditing, and other forms of monitoring and observation. (In fact, these same indicators are often used by attackers to gain an insight into a potential target.)

OPSEC also includes proper administrative and management processes that define how employees are hired/fired, how a system is safeguarded against internal attack, and how a successful attack is handled.

f. Describe "physical (environmental) security" as it relates to CS.

The following is taken from Inform IT, *Common Body of Knowledge (CBK)*.

The PS domain addresses threats, vulnerabilities, and countermeasures that can be utilized to physically protect an enterprise's resources and sensitive information. These resources include: people; the facility in which they work; and the data, equipment, support systems, media, and supplies they utilize.

In many ways, PS is very similar to information security. You have to assess the items that need protection, determine how they can be accessed, create protections and controls for these access methods, and then enforce and audit users as they operate the devices. There are five main assets that need protection: facility; supporting infrastructure (power, water, etc.); physical hardware; supplies and consumables; and people.

Each of these items has its own set of threats—some global (such as fire) and some related directly to the asset (such as theft). Using these threats as a guideline, a physical site should be selected and built according to a proper design.

Once the basic structure is selected, the proper controls need to be installed. These include identification screening using swipe cards, pin numbers, biometrics, or a human guard (to name a few options). In addition, proper controls must be placed on all components that leave a site. More than one business has fallen prey to attack as a result of what an attacker found in a trash can. Finally, a site should have some form of physical intrusion-detection to keep dishonest people from having direct access to the information-system hardware or supporting equipment. Unfortunately, even with all the proper precautions and controls in place, a site's PS can never be 100% guaranteed—think about natural disaster or a corrupt system administrator.

The following is taken from DOE M 205.1-4.

Access controls shall ensure that personnel granted unescorted physical access to the information, the information system, or human readable media have the appropriate access authorization, formal access approval, and need-to-know. Physical attack, which might compromise security, on those parts of the information system critical to security shall be deterred and detected.

The information system shall be protected by being constantly attended and under the control of a person that possesses proper access authorization, formal access approval, and need-to-know, or by physical protection, as prescribed for the classification level and category of the information, to restrict access to those with appropriate clearance, formal access approvals, and need-to-know.

The information system environment shall be capable of physically protecting the information system and components stored in a remote location by signaling the occurrence of fire, flood, power loss, and environmental control failures that might adversely affect information system operations.

g. Describe "security architecture and design" as they relate to CS.

The following is taken from the Inform IT, *Common Body of Knowledge (CBK)*.

The security architecture and models domain contains the concepts, principles, structures, and standards used to design, implement, monitor, and secure operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity, and availability.

Security architecture models are:

- The Bell-laPadula model basically defines security through confidentiality. Designed using the "no write down, no read up" model, security is maintained if a classified resource is accessed only by subjects with a clearance at that level or higher. This method works, but it relies on the assurance that access to the object is closely controlled.
- The Biba model focuses on integrity more than confidentiality. This model is built around two rules—no write up and no read down—which refer to the trust relationships that exist between subjects and objects. In short, no subject can depend on a less-trusted object, which restricts an unauthorized subject from changing or even accessing an object.
- The Clark-Wilson model emphasizes data integrity by restricting unauthorized access or improper modification by authorized users, and by maintaining internal and external consistency. This model is most often used to ensure that data modification is made with their integrity and consistency in mind.
- The most common model is based on the ACL, which is prevalent in most enterprise operating systems. This model uses a preexisting list of approved subjects, associated with objects. If a user wants access to a folder or file, the user's identification is checked against the ACL for that resource, and access is granted, as appropriate.

In addition to models, this domain also defines components of secure system architectures, including reference monitors, covert data channels, open versus closed systems, and various security principles and modes. Using combinations of these components, principles, and modes, a solid architecture can be designed and implemented that ensures the security of a company's data.

When a security system is designed, it should be evaluated using some form of security standard. The most common and well-known standards are described in the following list:

- Trusted Computer System Evaluation Criteria (TCSEC). TCSEC is more commonly known as the orange book, which is part of the famous Rainbow series. It is a U.S. government-founded security standard that critiques a system by its ability to separate users and data, the granularity of access control, and the trust of overall assurance of the system. Using these concepts, it then assigns a grade to the system.
- Information Technology Security Evaluation Criteria (ITSEC). This European standard focuses on loss of integrity, confidentiality, and availability. It is similar to TCSEC in many ways, with slight variations on how systems are evaluated and what is included in the evaluation.
- Common Criteria. This system evaluates products by version/environment and is not guaranteed against vulnerabilities. This standard is replacing ITSEC and TCSEC as an internationally agreed-upon method of evaluation. It is divided into three main parts: introduction and general model; security functional requirements; and security assurance. These all work together to critique a system and give it a grade or certification based on how it meets predefined requirements.
- One final standard that is growing in popularity is Internet Protocol Security (IPSEC), which is a communications standard found in firewalls, VPNs, and other communication devices/software. It controls what data can flow and how that data is transmitted, using a two-phase connection initialization process.

Security models and architecture should be at the foundation of how an information system is designed. Through the use of these concepts, a company can build a strong and reliable system that they can be confident using. However, it should be noted that no information system is 100% secure.

h. Describe "telecommunications and network security" as it relates to CS.

The following is taken from Inform IT, *Common Body of Knowledge (CBK)*.

The telecommunications and network security domain encompasses the structures, transmission methods, transport formats, and security measures used to provide integrity, availability, authentication, and confidentiality for transmissions over private and public communications networks and media.

This domain is one of the largest and most technical within the CBK. It includes the open system interconnection (OSI) model that defines how networked hardware and software

communicate. The OSI model's approach splits communication into seven distinct layers, each with a defined purpose, and each designed to interface with its neighboring layer(s).

The telecommunications and network security domain deals with the actual hardware used to connect information systems to each other—whether that's coax cable used for 10Base-2 or 10Base-5 wiring; the more commonly known categorized cabling schemes (Cat3, Cat5, Cat6, etc.) used for most Ethernet LANs; fiber lines that use light pulses; or a wireless network. Knowing each of these types of connectors and understanding where and how they can be used is important.

Know the foundations of networking; they start looking at the many types of network technologies, including the ring, tree, mesh, star, and linear. While some of these types have been phased out in recent years (ring networks, for example), new technologies are redefining existing types and creating new networking concepts. The recent development of the WLAN networking often becomes a dynamic situation as users move from one type of network to another seamlessly and without a break in communications.

The telecommunications and network security domain is best known by the actual devices and technologies used to support the increasingly networked world—the hubs, routers, switches, firewalls, and more that keep the data flowing. Degrees, certifications, and whole careers are built on understanding how these devices work together to pass a packet from one information system to another.

As a result, this domain also deals with the many safeguards and communications protocols that an administrator must employ to keep the data safe, secure, and error-free while it is in transport. This runs the gamut from the well-known transmission control protocol/internet protocol (TCP/IP) to the encrypted IPSEC used to secure many remote-access connections.

67. Safeguards and security personnel with the responsibility for CS must demonstrate a working level knowledge of information technology disciplines.

a. Describe the following technology elements and how they relate to CS:
- **Networks**
- **Hardware**
- **Software**
- **Databases**
- **Websites**
- **Programming**
- **Operating systems**

Networks

According to the DOE Glossary of Computer Terms, a network is an interconnection of three or more communicating entities and (usually) one or more nodes.

Hardware

According to DOE G 200.1-1, *Software Engineering Methodology* TOC, appendix A, hardware consists of the physical computer and other equipment used to process, store, or transmit computer programs or data.

Software

According to DOE G 200.1-1, appendix A, software consists of computer programs, procedures, and associated documentation and data pertaining to the operation of a software product or system.

Databases

According to the DOE Glossary of Computer Terms, databases consist of software that control the organizing, cataloging, locating, storing, retrieving, and maintaining of data in a database to maintain its integrity.

Websites

According to Princeton College, Word Net Search, a website is a computer connected to the Internet that maintains a series of web pages on the World Wide Web.

Programming

According to DOE G 200.1-1, appendix A, programming is the period of time in the software life cycle during which a software product is created from the design specifications and testing is performed on the individual software units.

Operating Systems

According to Princeton College, Word Net Search, operating systems consist of software that control the execution of computer programs and may provide various services.

Selected Bibliography and Suggested Reading

Code of Federal Regulations (CFR)

6 CFR 27, "Chemical Facility Anti-Terrorism Standards." January 1, 2009.

7 CFR 331, "Possession, Use, and Transfer of Select Agents and Toxins." January 1, 2009.

9 CFR 121, "Possession, Use, and Transfer of Select Agents and Toxins." January 1, 2009.

9 CFR 122, "Organisms and Vectors." January 1, 2009.

10 CFR 11.15, "Criteria and Procedures for Determining Eligibility for Access to or Control Over Special Nuclear Material." January 1, 2009.

10 CFR 74, "Material Control and Accounting of Special Nuclear Material." January 1, 2009.

10 CFR 95.19, "Changes to Security Practices and Procedures." January 1, 2009.

10 CFR 707, "Workplace Substance Abuse Programs at DOE Sites." January 1, 2009.

10 CFR 709, "Counterintelligence Evaluation Program." January 1, 2009.

10 CFR 710, "Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material." January 1, 2009.

10 CFR 710.5, "Definitions." January 1, 2009.

10 CFR 710.8, "Criteria." January 1, 2009.

10 CFR 710.9, "Action on Derogatory Information." January 1, 2009.

10 CFR 710.20, "Purpose of Administrative Review." January 1, 2009.

10 CFR 710.21, "Notice to the Individual." January 1, 2010.

10 CFR 710.22, "Initial Decision Process." January 1, 2009.

10 CFR 710.26, "Conduct of Hearings." January 1, 2009.

10 CFR 710.27, "Hearing Officer's Decision." January 1, 2009.

10 CFR 710.28, "Action on the Hearing Officer's Decision." January 1, 2009.

10 CFR 710.32, "Reconsideration of Access Eligibility." January 1, 2009.

10 CFR 712, "Human Reliability Program." January 1, 2009.

10 CFR 712.1, "Purpose." January 1, 2009.

10 CFR 712.10, "Designation of HRP Positions." January 1, 2010.

10 CFR 712.11, "General Requirements for HRP Certification." January 1, 2009.

10 CFR 712.17, "Instructional Requirements." January 1, 2009.

10 CFR 712.19, "Removal from HRP." January 1, 2009.

10 CFR 860, "Trespassing on DOE Property." January 1, 2009.

10 CFR 1016, "Safeguarding of Restricted Date." January 1, 2009.

10 CFR 1046, "Physical Protection of Security Interests." January 1, 2009.

10 CFR 1047, "Limited Arrest Authority and Use of Force by Protective Force Officers." January 1, 2009.

10 CFR 1047.4, "Arrest Authority." January 1, 2009.

10 CFR 1047.6, "Use of Physical Force When Making An Arrest." January 1, 2009.

10 CFR 1047.7, "Use of Deadly Force." January 1, 2009.

10 CFR 1049.6, "Exercise of Arrest Authority—Use Of Non-Deadly Force." January 1, 2009.
10 CFR 1049.7, "Exercise of Arrest Authority—Use Of Deadly Force." January 1, 2009.
32 CFR, Chapter XX, "Information Security Oversight Office, National Archives, and Records Administration." July 1, 2009.
32 CFR 2003, "National Security Information—Standard Forms." July 1, 2008.
41 CFR 101, "Federal Property Management Regulations." July 1, 2008.
42 CFR 73, "Select Agents and Toxins." October 1, 2008.
43 CFR 3150, "Offshore Oil and Gas Geophysical Exploration." October 1, 2009.
49 CFR 40, "Procedures For Transportation Workplace Drug And Alcohol Testing Programs." October 1, 2008.

CNSS Instruction No. 4009, National Information Assurance (IA) Glossary. June 2006.

Defense Advanced Research Projects Agency, *Perimeter Security Sensor Technologies Handbook*. 1997.

Director of Central Intelligence Directive (DCID) 6/9, Physical Security Standards for Sensitive Compartmental Information Facilities. November 18, 2002.

Executive Orders (EOs)

EO 12333, "United States Intelligence Activities." December 4, 1981.
EO 12564, "Drug-free Federal Workplace." September 15, 1986.
EO 12829, "National Industrial Security Program." January 6, 1993.
EO 12885, "Amendment to Executive Order No. 12826." December 14, 1993.
EO 12958, "Classified National Security Information." April 17, 1995.
EO 12968, "Access to Classified Information." August 4, 1995.

Federal; Information Processing Standards (FIPS)

FIPS 112, *Password Usage Standard*. May 30, 1985.
FIPS 181, *Automated Password Generator (APG)*. October 5, 1993.
FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*. February 2004.
FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. March 2006.

Federal Information Security Management Act (FISMA). 2002.

Federal Specification FF-L-2740, *Federal Specifications, Locks, Combinations*. October 12, 1989.

Information System Certification and Accreditation Process, Approval to Operate. June 27, 2001.

InformIT, *Common Body of Knowledge (CBK) Definitions*. March 1, 2004.

NAP-70.4, *Information Security*. July 2, 2010.

National Archives Records Administration General Records Schedule 18, *Security and Protective Services Record*. February 2008.

National Fire Protection Association (NFPA)**,** NFPA 101, "Life Safety Code." 2009.

National Institute of Standards and Technology (NIST)

NIST 800-21, Guidance for Implementing Cryptography in the Federal Government. December 2005.

NIST SP-800-30, Risk Management Guide for Information Technology Systems. Undated.

NIST SP-800-34, Contingency Planning Guide for IT Systems. June 2002.

NIST 800-37 Rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems. February 2010.

NIST SP-800-40, Creating a Patch and Vulnerability Management Program. November 2005.

NIST SP-800-47, Security Guide for Interconnecting Information Technology Systems. August 2002.

NIST SP-800-48, Guide to Securing Legacy IEEE 802.11 Wireless Networks. July 1, 2008.

NIST SP 800-60 Rev 1, Information Security. August 2008.

National Security Telecommunications and Information Systems Security (NSTISSI) No. 4011, *National Training Standard for Information Systems Security (INFOSEC) Professionals*. June 20, 1994.

Nuclear Regulatory Commission (NRC) Nuclear Regulation (NUREG)

NUREG-0006, Instructions for Completing Nuclear Material Transaction Reports. April 1, 2008.

NUREG-0007, Instructions for the Preparation and Distribution of Material Status Reports. January 1, 2009.

Office of Management and Budget (OMB) Circular A-11, *Planning, Budgeting, Acquisition of Capital Assets, Strategic Plans, Performance Plans*. August 2009.

Presidential Decision Directive**,** PDD 61, *U.S. Department of Energy Counterintelligence Program (*U). February 1998.

Price Anderson Amendment Act. 1988.

Princeton College, Word Net Search.

Public Law 83-703, *Atomic Energy Act of 1954*. August 30, 1954.

Sandia Laboratory, A Risk Assessment Methodology (RAM) for Physical Security.

Standard Form 86, *Questionnaire for National Security Positions*. September 1995.

Title III—Information Security, section 301, subchapter III, 3542, *Definitions*. 2002.

Underwriters Laboratory**,** UL 2050, *National Industrial Security Service Standard*. August 22, 2006.

United States Codes (U.S.C.)

18 U.S.C. 13, "Laws of States Adopted for Areas within Federal Jurisdiction." 1808.
42 U.S.C. 2121, "Authority of Commission." Undated.
50 U.S.C. 402a, "Counterintelligence and Security Enhancements Act of 1994." 1994.

U.S. Department of Energy Directives (Guides, Manuals, Orders, and Policies)

DOE Guide 200.1-1, *Software Engineering Methodology TOC*. May 21, 1997.
DOE Guide 413.3-15, *Department of Energy Guide for Project Execution Plan*s. September 12, 2008.
DOE Guide 473.2-1, *Guide for the Establishment of a Contingency Protective Force*, (archived). March 27, 2003.
DOE Manual 205.1-3, *Telecommunications Security Manua*l (OUO). April 17, 2006.
DOE Manual 205.1-4, *National Security System Manual*. March 8, 2007.
DOE Manual 205.1-5 Admin chg 2, *Cyber Security Process Requirements Manual*. August 12, 2008.
DOE Manual 205.1-6 Admin chg 2, *Media Sanitization Manual*. December 23, 2008.
DOE Manual 205.1-7 Admin chg 2, *Security Controls for Unclassified Information Systems Manual*. January 1, 2009.
DOE Manual 205.1-8 Admin chg 1, *Cyber Security Incident Management Manual.* January 8, 2009.
DOE Manual 231.1-1A chg 2, *Environment, Safety and Health Reporting Manual*. March 19, 2004.
DOE Manual 231.1-2, *Occurrence Reporting and Processing of Operations Information*. August 19, 2003.
DOE Manual 452.4-1A*,* Protection of Use Control Vulnerabilities and Design. March 11, 2004.
DOE Manual 470.4-1 chg 1, *Safeguards and Security Program Planning and Management*. March 7, 2006.
DOE Manual 470.4-2 chg 1, *Physical Protection* (archived). August 26, 2005.
DOE Manual 470.4-2A, *Physical Protection*. July 23, 2009.
DOE Manual 470.4-3 chg 1, *Protective Force*, (archived). August 26, 2005.
DOE Manual 470.4-3A, *Contractor Protective Force*. November 5, 2008.
DOE Manual 470.4-4, *Information Security*, (archived). August 26, 2005.
DOE Manual 470.4-4 chg 1, *Information Security* (archived). August 26, 2005.
DOE Manual 470.4-4A, *Information Security Manual*. January 16, 2009.
DOE Manual 470.4-5, *Personnel Security*. August 26, 2005.
DOE Manual 470.4-6 chg 1, *Nuclear Material Control and Accountability*. August 26, 2005.
DOE Manual 470.4-7, *Safeguards and Security Program References*, (archived). August 26, 2005.
DOE Manual 470.4-8, *Federal Protective Force*. July 15, 2009.

DOE Manual 471.1-1 chg 1, *Identification and Protection of Unclassified Controlled Nuclear Information*. October 23, 2001.
DOE Manual 471.2-2, *Classified Information Systems Security Manual*, (archived). August 3, 1999.
DOE Manual 471.2-3B, *Special Access Program Policies, Responsibilities, and Procedures (OUO)*. October 29, 2007.
DOE Manual 473.2-2 chg 1, *Protective Force Program Manual* (archived). December 20, 2001.
DOE Manual 475.1-1B, *Manual for Identifying Classified Information*. August 28, 2007.
DOE Manual 5632.1C-1 chg 1, *Manual for Protection and Control of Safeguards and Security Interests* (archived). April 10, 1996.
DOE Order 142.1, *Classified Visits Involving Foreign Nationals*. January 13, 2004.
DOE Order 142.3 chg 1, *Unclassified Foreign Visits and Assignments Program*. June 18, 2004.
DOE Order 151.1C, *Comprehensive Emergency Management System*. November 2, 2005.
DOE Order 205.1, *Department of Energy Cyber Security Management Program*, archived. March 21, 2003.
DOE Order 205.1A, *Department of Energy Cyber Security Management*. December 4, 2006.
DOE Order 206.1A, *Department of Energy Cyber Security Management*. December 4, 2006.
DOE Order 221.1A, *Reporting Fraud, Waste, and Abuse to the Office of Inspector General*. April 19, 2008.
DOE Order 226.1A, *Implementation of Department of Energy Oversight Policy*. July 31, 2007.
DOE Order 231.1A chg 1, *Environment, Safety, and Health Reporting*. June 3, 2004.
DOE Order 413.3A chg 1, *Program and Project Management for the Acquisition of Capital Assets*. July 28, 2006.
DOE Order 440.1B, *Worker Protection Program for DOE (including the National Nuclear Security Administration) Federal Employees*. May 17, 2007.
DOE Order 440.2B chg 1, *Aviation Management and Safety*. November 19, 2006.
DOE Order 457.1, *Nuclear Counterterrorism*. February 7, 2006.
DOE Order 470.2B, *Independent Oversight and Performance Assurance Program*. October 31, 2002.
DOE Order 470.3A, *Design Basis Threat Policy*, archived. November 29, 2005.
DOE Order 470.3B, *Graded Security Protection (GSP) Policy*. August 12, 2008.
DOE Order 470.4A, *Safeguards and Security Program*. May 25, 2007.
DOE Order 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*. June 30, 2000.
DOE Order 475.1, *Counterintelligence Program*. December 10, 2004.
DOE Order 3750.1 chg 6, *Work Force Discipline*. August 21, 1992.
DOE Order 3792.3, *Drug-free Federal Workplace Testing Implementation Program*. August 21, 1992.
DOE Order 5610.2 chg 1, *Control of Weapon Data*. September 2, 1986.

DOE Policy 205.1, *Departmental Cyber Security Management Policy*, (archived). May 8, 2001.
DOE Policy 226.1A, *Department of Energy Oversight Policy*. May 25, 2007.
DOE Policy 470.1, *Integrated Safeguards and Security Management Policy (ISSM)*. May 8, 2001.

DOE-STD-1171-2009, *Safeguards and Security Functional Area Qualifications Standard*. May 2009.

U.S. Department of Energy Other References

DOE Glossary of Computer Terms, Undated.
DOE CIO Guidance CS-6, *Plan of Action and Milestones Guidance*. September 2006.
DOE CIO Guidance CS-14, *Portable/Mobile Devices Guidance*. January 2007.
DOE CIO Guidance CS-20, *Security Architecture*. February 2007.
DOE CIO Guide 205.1-2, *Certification and Accreditation Guide*. March 2006.
DOE, Configuration Management (TMR-8), Cyber Security Technical and Management Requirements. August 10, 2007.
DOE Cyber Security Awareness and Training Program Plan and Essential Body of Knowledge (EBK). January 2009.
DOE Headquarters Security Quick Reference Book. October 2008.
DOE Office of Counterintelligence, *Hosting Foreign Nationals at DOE Sites*. Undated.
DOE Organization Act, Section 661. 1977.
DOE Program Cyber Security Plan. May 9, 2007.
DOE Security Plan for Non-Possessing Facilities. Undated

U.S. Joint Forces Command (USJFCOM) Fact Sheet, *Joint Conflict and Tactical Simulation*. Undated.

U.S. National Archives and Records Administration, *Controlled Unclassified Information Framework*. September 16, 2009.

Safeguards and Security Qualification Standard Reference Guide

OCTOBER 2010